El fraude en el entorno cibernético

Asociación española de gestión de riesgos y seguros AGERS

Índice

Agradecimientos 3

1 Introducción 4

1.1. Objetivo de esta guía 4
1.2. ¿Por qué es importante abordar el fraude cibernético hoy? 4
1.3. Evolución del fraude digital: del phising a la IA generativa 5
1.4. Alcance del trabajo: Ciberriesgo + *Seguro Crime* 5

2 El fraude en general 5

3 El fraude cuando hablamos del entorno cibernético 7

3.1. ¿Qué entendemos por fraude cibernético? 7
3.2. El factor humano: el eslabón más débil 7
3.3. Tipologías frecuentes de fraude en el mundo digital 8
3.4. Ejemplos de casos reales 10

4 Anatomía de un fraude: como se prepara y ejecuta 11

4.1. La fase de reconocimiento y recolección de información 12
4.2. Técnicas de ingeniería social más utilizadas. Canales de ataque: email, teléfono, redes sociales, etc. 12
4.3. De la intrusión al impacto: consecuencias reales 13

5 Prevención y mitigación 14

5.1. Formación y concienciación: claves para reducir el riesgo 14
5.2. Simulaciones y entrenamiento: cómo preparar a la organización 19
5.3. Controles técnicos y organizativos recomendados 15
5.4. Procedimientos internos y roles responsables 15

6 La transferencia del riesgo: seguros aplicables 17

6.1. Seguro *crime* 17
6.2. Tipos de fraude cubiertos 18
6.3. Coberturas básicas 19
6.4. Otras coberturas 20
6.5. Exclusiones 21
6.6. Ventajas estratégicas del seguro *crime* 22
6.7. Tendencias del seguro 23
6.8. Tendencias del mercado 25
6.9. Diferencias del seguro *crime* vs ciber 26

7 Casos prácticos 27

7.1. Pago a proveedor 28
7.2. Fraude en la entrega de mercancía 29
7.3. Fraude del CEO 31

8 Conclusiones del grupo de trabajo 33

9 Sobre la comisión de riesgos tecnológicos de Agers 35

10 Entidades colaboradoras 36

Agradecimientos

Expertos participantes

Queremos agradecer su trabajo, dedicación y apoyo a los profesionales que en colaboración con AGERS han hecho posible de esta guía:

Coordinadora y líder del proyecto.
Belén Medina

Juan Ramón Claver

Álvaro González

Juan Gayá Soler

África Sánchez

Raquel Caballero

Juan Miguel García Mediavilla

David Martínez Suárez

Laura Blanco Pérez

Ignacio Reclusa

Francisco de Borja de Corral Mateos

Pedro Morato

1. Introducción

El seguro ***Crime*** ha evolucionado desde su enfoque tradicional — centrado en la infidelidad de empleados y la apropiación indebida— hacia una solución integral **que cubre tanto el fraude interno como el externo en entornos altamente digitalizados.** La creciente dependencia de las organizaciones de plataformas tecnológicas, junto con el auge de las técnicas de ingeniería social (BEC/"fraude del CEO", *phishing*, suplantación en canales colaborativos), ha ampliado el perímetro de exposición y ha trasladado el fraude a un plano donde **la identidad y la verificación operativa son determinantes.**

En este contexto, el seguro *Crime* se consolida como una herramienta esencial de transferencia del riesgo, complementaria del seguro Ciber: mientras Ciber prioriza la respuesta técnica forense y la gestión de crisis ante ataques, Crime protege la pérdida patrimonial directa (dinero, valores, activos) causada por la deshonestidad o el engaño —ya provenga de empleados o de terceros que manipulan procesos de pago o relaciones con proveedores y clientes.

Este documento analiza las coberturas principales (infidelidad, hurto, estafa, falsificación, fraude informático y transferencias fraudulentas), las extensiones relevantes (gastos de investigación/forense, reconstitución de sistemas, custodia de fondos de clientes, fraude por deepfakes/IA, deshonestidad de terceros), y las exclusiones habituales que delimitan el alcance de la póliza; asimismo, expone las ventajas estratégicas (cultura ética, trazabilidad, protección reputacional, ventaja competitiva) y las tendencias del mercado (capacidad, franquicias, límites, proceso de suscripción y controles exigidos), con especial foco en complementariedad entre *Crime* y Ciber.

1.1 Objetivo de esta guía

El objetivo de esta guía es proporcionar una visión integral del fraude digital, analizar sus tipologías actuales, comprender cómo se articulan y transfieren estos riesgos mediante el seguro Crime, y ofrecen recomendaciones prácticas para mejorar la resiliencia organizativa.

1.2 ¿Por qué es importante abordar el fraude cibernético hoy?

La digitalización de procesos, el trabajo en remoto, el uso intensivo de capacidades colaborativas y la explotación de la inteligencia artificial han creado un entorno en el que los ataques se multiplican en sofisticación y frecuencia. El fraude cibernético es ya un riesgo financiero, no solo tecnológico.

1.3 Evolución del fraude digital: del phishing a la IA generativa

Los ataques han pasado de simples correos engañosos a elaboradas campañas apoyadas en herramientas de IA generativa capaces de imitar voces, rostros, documentos y comportamientos. Los *deepfakes* y la automatización del engaño elevan la probabilidad de éxito de los delincuentes.

1.4 Alcance del trabajo: Ciberriesgo + Seguro *Crime*

El documento aborda:

- Tipologías de fraude digital.
- Papel de la ingeniería social.
- Mecanismos de prevención.
- Coberturas del seguro Crime.
- Casos reales que ilustran el impacto de estos incidentes.

2. El fraude en general

El concepto de fraude en el contexto de una póliza *Crime* es amplio, ya que al primer germen del ramo, nacido en 1853 para cubrir las pérdidas financieras por actos deshonestos de empleados, se han ido añadiendo coberturas afines a este concepto original que todos podemos asociar automáticamente.

De esta forma, cuando tomamos en consideración una póliza Crime, el fraude se define como un catálogo de actos ilícitos patrimoniales cometidos por empleados o terceros que ocasionan una pérdida económica cuantificable sobre bienes asegurados, que pueden ser bienes físicos, valores, dinero (monedas y billetes de curso legal) o incluso lingotes de oro y plata.

Si clasificamos las tipologías frecuentes de fraude recogidas en una póliza *Crime* podemos atender a dos criterios: El actor y el canal o entorno en el que se desarrolla el siniestro.

Fraude según el actor

Si atendemos al actor, podemos diferenciar entre fraude interno o externo.

- Fraude interno (Acto de infidelidad de empleado): Aquí incluiríamos cualquier acto perpetrado por un empleado, como autor o cómplice.

- Fraude externo (Acto fraudulento de tercero): Aquí incluiríamos cualquier acto perpetrado por un tercero, sin complicidad o cooperación alguna de un empleado.

Fraude según el canal o entorno

Si atendemos al canal, nos encontramos con fraudes cometidos en entornos físicos y fraudes cometidos en entornos cibernéticos.

- Crime físico:

- Robo/Hurto/Destrucción de equipos: Se refiere a la pérdida o daño de equipos físicos de la empresa.

- Robo/Hurto/Destrucción de materiales o mercancías: Orientado a materias primas, mercancía almacenada o en tránsito, o bienes destinados a la actividad que son sustraídos o dañados.

- Robo/Hurto/Destrucción de dinero en metálico: Comprende la pérdida directa sufrida por la destrucción física o desaparición de dinero o valores, situados en los locales o fuera de ellos, y bajo custodia autorizada.

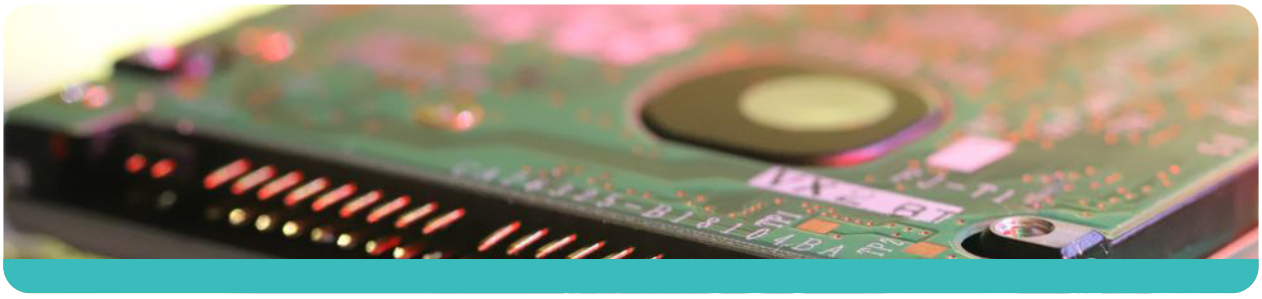
- Crime financiero en entorno cibernético:

- Transferencia fraudulenta de fondos por parte de un empleado: Se refiere a la transferencia, pago o entrega de dinero o valores desde una cuenta del asegurado, realizada fraudulentamente por un empleado mediante instrucciones dadas a la entidad financiera, sin conocimiento o consentimiento de la dirección de la empresa.

- Transferencia fraudulenta de fondos por parte de un tercero: Comprende la transferencia fraudulenta de fondos, siempre sin complicidad o cooperación de un empleado. En términos prácticos, cubre el supuesto en que un actor externo logre que se curse una instrucción fraudulenta a la entidad financiera o se produzca un desvío no consentido de dinero o valores desde cuentas del asegurado.

- Fraude de ingeniería social: Es un acto fraudulento de terceros cometido por un impostor, que suplanta a un proveedor, cliente o directivo, que engaña a un empleado para hacer una transferencia, pagar o entregar bienes asegurados. No es necesario que haya una intrusión técnica en el sistema, lo esencial es que haya una manipulación sobre una persona.

- Fraude con intrusión en sistemas: Corresponde a pérdidas por fraude derivadas de acceso no autorizado o uso indebido de sistemas informáticos para sustraer fondos o bienes.



3. El fraude cuando hablamos del entorno cibernético

3.1 ¿Qué entendemos por fraude cibernético?

El Fraude cibernético es un acto deshonesto intencionado realizado por un empleado (interno) o un tercero (externo) a través de medios digitales para obtener beneficios financieros. El autor del fraude quiere causar un daño y conseguir un beneficio ilícito.

Cualquier actividad engañosa o ilícita que se lleve a cabo a través de medios digitales o plataformas en línea, con el objetivo de obtener beneficios financieros, acceder a información confidencial o causar daños a individuos o empresas aprovechando la tecnología y las vulnerabilidades de los sistemas informáticos o engañando a los usuarios.

Por ese motivo, los costes que deben invertir las empresas para protegerse también se incrementan. Ya que deben invertir en herramientas de detección de fraudes, medidas de protección y también programas de capacitación para empleados que vayan más allá de los simples consejos de ciberseguridad.

3.2. El factor humano: el eslabón más débil

Los errores humanos son responsables del 95% de los eventos de ciberseguridad, lo que supone que más de 9 de cada 10 de los incidentes tienen como origen el factor humano. El factor humano se configura, así como un punto crítico de vulnerabilidad en las organizaciones.

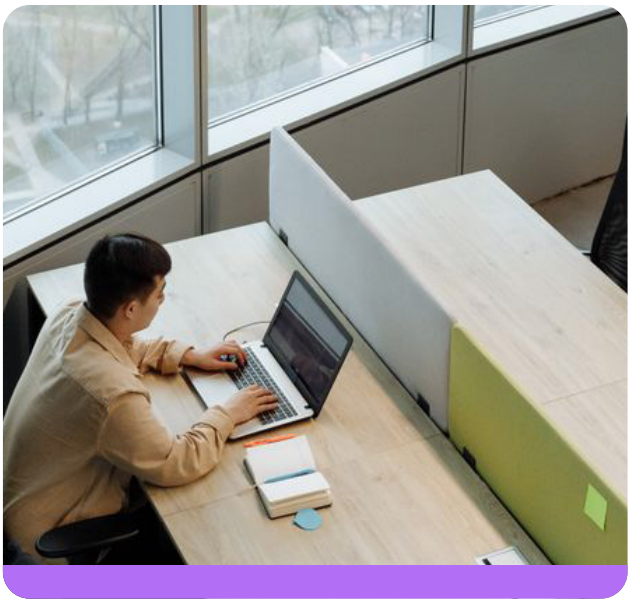
En este contexto, no es suficiente contar exclusivamente con capacidades tecnológicas y equipos de IT, es necesario incorporar la formación y concienciación de (empleados, directivos, clientes...) como elemento clave para prevenir ciberamenazas y mitigar su impacto económico.

La formación de los empleados debe ser una prioridad estratégica, y es clave el desarrollo de capacidades internas que permitan identificar y escalar posibles amenazas, contribuyendo a una defensa más robusta frente a ciberataques.

Este enfoque empieza con la formación y una buena concienciación en materia de ciberseguridad.

El factor humano es especialmente susceptible a técnicas de ingeniería social, que los ciberdelincuentes emplean para manipular comportamientos y eludir controles establecidos.

Ofrecer cursos adaptados a las necesidades de cada empleado constituye, por tanto, una herramienta fundamental para prevenir este tipo de riesgos. Una formación personalizada, según sus conocimientos y su nivel, permite optimizar su capacidad para identificar, prevenir y responder a las potenciales amenazas.



3.3. Tipologías frecuentes de fraude en el mundo digital

Las tipologías de fraude descritas a continuación representan las formas más habituales en las que se materializan los ataques en entornos digitales. Si bien presentan características específicas, en la práctica todas ellas comparten un elemento común: su ejecución se apoya en técnicas de ingeniería social dirigidas a manipular comportamientos y eludir controles. Estos mecanismos serán desarrollados posteriormente en el capítulo 4 donde se analiza en detalle la secuencia y dinámica de los ataques.

- **Fraude del CEO:** En este tipo de fraude, el atacante, haciéndose pasar por un alto cargo de la Compañía (por ejemplo, el Director General o Director Financiero), envía un correo electrónico falso a un empleado autorizado para realizar pagos, pidiéndole que pague una factura falsa, que realice una transferencia bancaria o envíe información fiscal confidencial. Además, a estos correos se les suele imprimir un aire de urgencia como medida de presión hacia el colaborador. Este fraude es particularmente peligroso porque el atacante se basa en la autoridad del CEO para engañar al empleado, y, por tanto, muchos de ellos no se plantearán cuestionar una orden de la Dirección y realizarán inmediatamente lo que se les ha pedido.

- ***Phishing:*** Esta forma de estafa consiste en obtener información confidencial de forma fraudulenta haciéndose pasar por una empresa de confianza y pidiendo datos personales o financieros. Este tipo de fraude se produce mediante correo electrónico, redes sociales o incluso llamadas. Los ciberdelincuentes confían en el hecho de que la gente está ocupada y, a primera vista, estos correos electrónicos falsos parecen ser legítimos, por lo que es muy probable que los destinatarios se crean lo que está escrito en ellos y hagan lo que se les pide (hacer clic en un enlace o descargar un fichero adjunto).

- ***Spear Phishing:*** Es cuando el phishing va dirigido contra un objetivo específico, ya sea un individuo o grupo. Estos ataques están diseñados para tener un mayor porcentaje de éxito que los ataques de phishing más generales, ya que son más personalizados y se basan en detalles realistas.

- ***Vishing:*** (combinación de las palabras voice -voz en inglés- y phishing) Es una estafa telefónica en la que los delincuentes, haciéndose pasar por un proveedor, cliente u otro empleado, intentan engañar a la víctima para que divulgue información personal, financiera o de seguridad o bien para que les transfiera dinero.

- ***Pharming:*** A diferencia del phishing, el pharming manipula el tráfico de un sitio web para redireccionar a los usuarios a sitios maliciosos pero con un aspecto similar. Una vez dentro, se produce la descarga de un software que roba información sensible como contraseñas o datos bancarios.

- **Carding:** El carding se basa en el uso fraudulento de tarjetas de crédito de otras personas. Normalmente el proceso comienza con una llamada, el operador solicita un número de tarjeta de crédito o bien mediante un email. Una vez en poder del atacante, este realiza compras de manera reiterada y paulatina para no levantar sospechas. Si además se trata de tarjeta de empresa, se tiene un menor control de los gastos que se producen en la misma, dado que no se suele tener acceso a la cuenta.

- **Fraude por manipulación de cuentas bancarias:** Alteración de detalles bancarios para desviar fondos. Una empresa es contactada por una persona que dice pertenecer a una compañía proveedora de servicios. El atacante solicita que se modifiquen los datos bancarios de un pago (es decir, los datos del beneficiario de la cuenta bancaria), porque han realizado un cambio de cuenta o de banco, para ese pago como para facturas futuras. La nueva cuenta sugerida está controlada por el atacante

- **Deepfakes y uso de IA para suplantación:** Uso de IA para crear falsificaciones de voz o video. Los ataques deepfake utilizan archivos de vídeo, imagen o voz manipulados mediante un software de inteligencia artificial, de modo que parezcan auténticos y reales, con el objetivo de engañar a personas o sistemas. Con esta técnica, los atacantes generan contenidos falsos que imitan a la perfección a personas reales. Esta tecnología se basa en redes neuronales y deep learning, que permiten generar contenido sintético imitando expresiones faciales, voces y gestos de forma muy realista, y permite que, a través del uso del rostro y la voz de personas de confianza, las víctimas sean convencidas para transferir dinero, compartir datos sensibles u otorgar accesos no autorizados. Los atacantes se pueden hacer pasar por ejecutivos, empleados o clientes, lo que genera una gran vulnerabilidad a las empresas. Más allá de las pérdidas financieras directas, el daño reputacional puede ser igual o más grave, ya que un solo vídeo manipulado puede dañar la reputación de la empresa de forma irreversible.

3.4. Ejemplos de casos reales

En las siguientes líneas nombramos algunos de los incidentes que se han hecho públicos en los últimos años. Como se puede ver, la tipología es variada y los impactos muy significativos:

1. **Ubiquiti – $46,7 millones:** La empresa de redes Ubiquiti sufrió un fraude, en el que los atacantes se hicieron pasar por un proveedor legítimo para solicitar transferencias a cuentas bancarias controladas por ellos.

2. **Google y Facebook – $121 millones:** Caso muy famoso en el que el estafador Evaldas Rimasauskas creó una empresa falsa con el nombre "Quanta Computer" (nombre idéntico al de un proveedor real) e hizo facturas falsas a Google y Facebook.

3. **Toyota Boshoku – $37 millones:** En 2019, una filial de Toyota fue víctima de un ataque donde se persuadió a un ejecutivo financiero para que cambiara las instrucciones de pago y enviara dinero a una cuenta fraudulenta.

4. **Scoular Co. – $17,2 millones:** En este caso, los atacantes se hicieron pasar por ejecutivos de la empresa y urgieron una transferencia relacionada con una supuesta adquisición en China, con un argumento creíble para evitar controles internos.

5. **Obinwanne Okeke – $11 millones:** Okeke lideró una red de fraude BEC coordinada mediante phishing donde se consiguieron credenciales de ejecutivos y luego se enviaron instrucciones de transferencia falsas.

6. **Real estate en París – €38 millones:** Una empresa inmobiliaria en París fue víctima de una banda internacional que, mediante fraude de CEO / BEC, consiguió desviar 38 millones de euros.

Creemos que es de especial interés explicar en detalle un fraude deepfake contra Arup en Hong Kong en 2024. En enero de ese año, un empleado de la oficina de Arup en Hong Kong recibió un mensaje (por *email* o *WhatsApp*) del supuesto director financiero (CFO) con sede en Reino Unido, pidiéndole que participara en una transacción confidencial. Le invitaron a una videoconferencia con varias personas, todos ejecutivos de la empresa, para discutir esta operación. En esa videollamada, todos los participantes, incluyendo el supuesto CFO, eran en realidad *deepfakes*, tanto las imágenes y como las voces eran generadas por inteligencia artificial y manipuladas para parecer empleados reales.

Tras la videollamada con su "CFO", el empleado realizó lo que se le había solicitado, unas 15 transferencias diferentes a 5 cuentas bancarias en Hong Kong, por un total de HK$ 200 millones (unos 25,6 millones de USD).

Más adelante, el empleado contactó con la sede central de Arup y se descubrió que había sido víctima de un engaño, la policía de Hong Kong abrió una investigación, aunque no se conoce de detenciones concretas por este incidente.

Lo interesante del tema es cómo se usó la tecnología (ingeniería social + *deepfake*), ya que los estafadores usaron IA para clona rostros y voces a partir de vídeos públicos. Reutilizaron

grabaciones, seguramente conseguidas de conferencias, presentaciones públicas, etc., para recrear digitalmente al CFO y otros miembros de la empresa. Según algunas fuentes, la videollamada no fue en directo sino pregrabada teniendo los "ejecutivos" frases preparadas para la reunión, y tras dar las instrucciones básicas, luego siguieron por email con los detalles bancarios para realizar las transferencias. Aunque Arup declaró que su estabilidad financiera y operaciones no se vieron afectadas y que sus sistemas internos no habían sido comprometidos, el caso pone de manifiesto un riesgo crítico para la confianza interna y externa, y demostró también que incluso grandes empresas con controles sofisticados pueden ser víctimas si no tienen protocolos específicos para autenticar reuniones virtuales de alto riesgo.

Nos encontramos en un contexto en el que es imprescindible cuestionarlo todo y, especialmente, reforzar los controles e implantar medidas adicionales cuando se recibe una solicitud de pago confidencial y/o urgente. Resulta fundamental establecer una doble verificación a través de un canal alternativo, comprobar la identidad del solicitante y realizar la correspondiente consulta o comprobaciones necesarias. Esta política debe ser de obligado cumplimiento para todos los empleados de la empresa.

4. Anatomía de un fraude: cómo se prepara y ejecuta

El fraude, en sus múltiples manifestaciones, representa uno de los mayores desafíos para la integridad y la seguridad de las organizaciones en la era digital. La sofisticación de las técnicas empleadas por los delincuentes, unida a la creciente dependencia de la tecnología y la conectividad global, ha elevado el riesgo y el impacto potencial de estos incidentes.

Comprender en profundidad la anatomía de un fraude, desde su fase inicial de reconocimiento hasta la explotación final, es esencial para anticipar, detectar y prevenir incidentes que pueden comprometer tanto los activos económicos como la reputación y la confianza de empresas y profesionales. Se presenta, por lo tanto, como una herramienta fundamental para la prevención, el conocimiento y análisis de las diferentes metodologías, formas y usos seguidas por aquellos que, con un objetivo lúdico o lucrativo, pretenden realizar un fraude tomando como base el entorno digital.

Este capítulo no tiene por objeto describir nuevamente las tipologías de fraude (ya analizadas en el apartado 3.3), sino explicar cómo estas se articulan en la práctica a través de patrones comunes de preparación y ejecución.

En este sentido, se presenta un enfoque práctico orientado a identificar vulnerabilidades, reforzar controles internos y comprender cómo técnicas como la ingeniería social y el uso de herramientas avanzadas (IA, deepfakes) se integran en las distintas fases del ataque.

4.1. La fase de reconocimiento y recolección de información

Comprender la anatomía de un fraude es esencial para anticiparlo, detectarlo y, sobre todo, prevenirlo. Aunque cada caso varía, en la mayoría los criminales siguen un patrón: reconocimiento, preparación, interacción manipulada y explotación final.

La etapa del reconocimiento comienza con una fase "silenciosa" y no visible. Los estafadores recopilan toda la información posible para comprender a quién atacarán y cómo hacerlo con la mayor probabilidad de éxito. Buscan cualquier detalle que permita construir un perfil preciso de la víctima (sea una persona o una organización):

- Datos personales: nombre, dirección, cumpleaños, DNI y, MUY importante, los perfiles en redes sociales. De hecho, entre las fuentes más utilizadas destacan tanto las redes sociales personales como las profesionales (LinkedIn, Facebook, X, Instagram, etc.).
- Información laboral: cargo, responsabilidades, relación con proveedores, nivel de autoridad en pagos o accesos.
- Datos técnicos: dominios, direcciones IP, servicios expuestos, proveedores tecnológicos, softwares utilizados.
- Estructura organizativa: jerarquías, departamentos, nombres de directivos y responsables.
- Hábitos de comunicación: horarios habituales, tono de correos, formato de firmas electrónicas, plantillas corporativas.

4.2. Técnicas de ingeniería social más utilizadas. Canales de ataque: email, teléfono, redes sociales, etc

El Fraude de Ingeniería Social se basa en la manipulación psicológica. El objetivo del atacante no es romper un sistema tecnológico, sino convencer a una persona para que realice una acción perjudicial, como la de entregar datos, ejecutar un pago o permitir acceso a sistemas. Se basa en la interacción humana y las técnicas que se emplean son muy variadas y pueden incluir correos electrónicos que parecen ser enviados por empleados, proveedores o clientes, llamadas telefónicas, mensajes de texto, USB infectados con malware y redes sociales.

Las principales técnicas utilizadas —como phishing, spear phishing, vishing, smishing o deepfakes, descritas previamente en el apartado 3.3— se emplean de forma combinada en función del objetivo y del nivel de sofisticación del ataque.

En lugar de constituir eventos aislados, estas técnicas se integran en una secuencia estructurada que incluye:

- Recopilación previa de información,
- generación de confianza mediante suplantación,
- introducción de urgencia o presión
- y ejecución de la instrucción fraudulenta.

Por tanto, el elemento diferenciador no es tanto la tipología concreta, sino la forma en la que estas se orquestan dentro del proceso de ataque.

4.3. De la intrusión al impacto: consecuencias reales

Una vez que el atacante logra manipular a la víctima o acceder a los sistemas, comienza la fase de explotación. Aquí se materializa el fraude y se desencadenan sus consecuencias:

1. Pérdidas financieras directas (transferencias fraudulentas, pagos manipulados a cuentas bancarias controladas por estafadores, robo de activos e incluso una interrupción operativa con impacto).

2. Daño reputacional con la pérdida de confianza de clientes, empleados, proveedores y accionistas que puede ser más costosa incluso que el propio impacto económico directo y que muchas veces no se tiene en cuenta a la hora de evaluar el riesgo.

3. Pérdida o exposición de información sensible como datos personales, secretos comerciales, estrategias empresariales o credenciales de acceso pueden ser robados y vendidos o utilizados para extorsión.

4. Sanciones regulatorias, especialmente en casos de incumplimientos relacionados con el RGPD, PCI-DSS u otras normativas sectoriales.

5. Costes de recuperación

6. Impacto emocional y organizativo, la culpa, la presión y el estrés sobre empleados implicados puede ser significativo, especialmente cuando el fraude se apoya en técnicas de manipulación emocional.

Y por desgracia, tenemos muchos ejemplos reales a explicar para ver la magnitud de lo que nos podemos encontrar. Comprometer el correo electrónico empresarial (lo encontraremos muchas veces en inglés con las siglas BEC -*Business Email Compromise*-) es especialmente atractivo para los atacantes porque aprovecha la confianza y la "normalidad" del uso de este correo y es fácil hacer pasar un *email* falso por una comunicación legítima de negocio. Muchas de estas estafas se apoyan en una ingeniería social muy paciente, y es que no basta con un *email*, hay elaboración de facturas falsas, creación de entidades ficticias ("empresa clon"), uso de documentos legales falsos, etc.

5. Prevención y mitigación

La prevención del fraude cibernético debe integrarse en el marco de gobernanza del riesgo de la organización, alineando personas, procesos, controles y responsabilidades.

La gestión eficaz de los riesgos cibernéticos se ha convertido en una prioridad estratégica para las organizaciones, especialmente ante el aumento de fraudes digitales y ataques dirigidos a procesos críticos como los pagos. La prevención y mitigación de estos riesgos no pueden abordarse únicamente desde la perspectiva tecnológica; requieren una visión integral que combine la capacitación de las personas, la definición de procesos sólidos y la implantación de controles técnicos y organizativos alineados con los estándares internacionales. La afección de los riesgos cibernéticos es, por tanto, transversal y afecta a todas las áreas de la compañía. Si bien es cierto que los objetivos fundamentales son las personas de los departamentos de tesorería, administración o finanzas de las empresas, no debemos olvidar que cualquiera de nosotros, en el seno de nuestras organizaciones, puede ser objeto y puerta de entrada de este tipo de fraudes.

Este texto explora los pilares fundamentales para reducir la probabilidad y el impacto de incidentes cibernéticos: la formación continua y la concienciación del personal, la realización de simulaciones y entrenamientos prácticos, la implementación de controles robustos y la definición clara de procedimientos y roles dentro de la organización. A través de un enfoque práctico y orientado a la realidad empresarial, se ofrecen recomendaciones y buenas prácticas para fortalecer la resiliencia frente a amenazas cada vez más sofisticadas, subrayando la importancia de una cultura de seguridad compartida y de la colaboración entre todas las áreas implicadas.

La prevención de los riesgos cibernéticos no se limita exclusivamente a la tecnología, sino que exige un enfoque equilibrado basado en personas, procesos y controles. El objetivo es reducir la probabilidad de que se produzcan incidentes y, en caso de que ocurran, minimizar su impacto. En el ámbito del fraude digital y de los ataques dirigidos a procesos críticos —como los pagos—, la estrategia debe apoyarse en una formación adecuada, procedimientos sólidos y controles técnicos y organizativos eficaces.

5.1. Formación y concienciación: claves para reducir el riesgo

El factor humano sigue siendo el eslabón más débil en la cadena de seguridad. Por ello, la educación y concienciación son esenciales para disminuir la exposición al fraude:

- **Programas continuos de formación:** No basta con sesiones puntuales; se requiere un plan anual que incluya actualizaciones sobre nuevas técnicas de fraude (*phishing*, ingeniería social, *spoofing*).

- **Enfoque práctico:** Explicar cómo se materializan los riesgos en el día a día del negocio (por ejemplo, correos falsos solicitando pagos urgentes).

- **Indicadores de alerta:** Capacitar a los empleados para identificar señales de fraude (dominios sospechosos, cambios en cuentas bancarias, lenguaje inusual).

- **Cultura de reporte:** Fomentar que cualquier duda se comunique sin penalización, creando un entorno donde la seguridad es responsabilidad compartida.

5.2. Simulaciones y entrenamiento: cómo preparar a la organización

La teoría no es suficiente; la organización debe ensayar escenarios reales para garantizar la respuesta adecuada:

- **Simulaciones de phishing:** Envío controlado de correos falsos para medir la reacción y reforzar la formación.

- **Role-playing en procesos críticos:** Simular solicitudes fraudulentas de pago para evaluar la adherencia a protocolos.

- **Evaluación periódica:** Medir resultados y ajustar los planes de formación según las brechas detectadas.

- **Integración con planes de continuidad:** Asegurar que los ejercicios incluyan la coordinación con áreas como Finanzas, IT y Compliance.

5.3. Controles técnicos y organizativos recomendados

Los controles deben ser proporcionales al riesgo y alineados con estándares como ISO 27001 o NIST:

- **Autenticación y políticas de contraseñas robustas:** Uso de MFA (*Multi-Factor Authentication*) en accesos críticos.

- **Segregación de funciones y segmentación de privilegios:** Ningún empleado debe tener control total sobre la autorización y ejecución de pagos.

- **Doble verificación en pagos:** Confirmación por una segunda persona antes de aprobar transferencias, especialmente internacionales.

- **Alertas automatizadas:** Sistemas que detecten cambios en cuentas bancarias o patrones inusuales en pagos.

- **Registro y trazabilidad:** Auditoría completa de todas las operaciones para facilitar investigaciones.

5.4. Procedimientos internos y roles responsables

La prevención requiere claridad organizativa:

- **Políticas documentadas:** Procedimientos para la validación de pagos, gestión de incidentes y comunicación interna.

- **Asignación de roles:**
  - *Risk Manager:* Supervisión del marco de control y análisis de riesgos emergentes.
  - *Finance:* Cumplimiento estricto de protocolos de autorización.
  - *IT Security:* Implementación y mantenimiento de controles técnicos.
  - *Compliance:* Verificación del alineamiento con normativas y estándares.

- **Escalamiento definido:** Rutas claras para reportar incidentes y activar planes de respuesta.

Finalmente, tanto el Gerente de Riesgos como el responsable de Seguridad de la Información deben mantenerse en una posición de vanguardia, atentos a la evolución constante de la sociedad y de las amenazas emergentes. Conocer y compartir mejores prácticas, fomentar foros de intercambio con otros profesionales que ya han implantado medidas efectivas, y aprender de quienes lideran los nuevos desarrollos en este ámbito contribuye de manera decisiva a lo esencial: la prevención de este tipo de fraudes..

6. La transferencia del riesgo: seguros aplicables

Los seguros *Crime* están en el mercado desde hace varias décadas siendo considerado un producto "maduro".

La cobertura con la que comenzó a comercializarse este seguro fue la de fidelidad de empleados, cubriendo las apropiaciones indebidas de bienes de la empresa cometidas por trabajadores del asegurado. Debido a ello, el ramo *Crime* estaba inicialmente muy orientado a sectores especialmente expuestos a estos actos, como entidades bancarias, transportadores de fondos o empresas relacionadas con el juego.

La digitalización de las compañías supuso una mayor exposición a este tipo de eventos, haciendo que este seguro se extendiera a otros sectores.

El seguro *Crime* actual, además de seguir dando las coberturas tradicionales con las que históricamente se le asocia, se diseña para abordar los retos derivados de la mayor dependencia de las empresas respecto de las redes tecnológicas, cubriendo lo que podríamos llamar ciber *Crime*.

En este contexto, el seguro *Crime* se presenta como una herramienta esencial de transferencia del riesgo, al ofrecer protección frente a infidelidades, fraudes informáticos y manipulaciones digitales que impactan directamente en los activos de la empresa. A diferencia del seguro ciber, más orientado a la respuesta frente a incidentes tecnológicos externos, el seguro *Crime* aporta un enfoque específico centrado en el fraude económico, tanto en su vertiente tradicional como en su evolución hacia el entorno digital.

6.1. Seguro *Crime*

El seguro Crime protege a la empresa frente a pérdidas financieras directas derivadas de actos deshonestos o fraudulentos cometidos por empleados (fraude interno) o terceros (fraude externo).

Con carácter general, el mercado ofrece cobertura sobre bienes propiedad del asegurado y, en determinados casos, sobre bienes de terceros bajo su control o custodia, siempre dependiendo de la redacción específica de la póliza y de las extensiones contratadas.

6.2. Tipos de fraude cubiertos

Fraude Interno

Se consideran como tal los actos cometidos por un empleado, tales como robo, falsificación, transferencia fraudulenta de fondos o fraude informático.

Ejemplos:

- Proveedores ficticios.
- Fraude de nóminas.

Con carácter orientativo, los *wordings* de mercado suelen contemplar:

- La pérdida directa sufrida por el asegurado (fondos propios), siempre que derive de un acto cubierto y debidamente probado.
- Robo de propiedades, metálico o bienes del asegurado perpetrados por un empleado.
- Robo de bienes de clientes bajo custodia del asegurado cometido por un empleado, cuando exista la extensión expresa en el *wording.*
- Gastos y honorarios razonables de los profesionales encargados de investigar las circunstancias de pérdida cubierta o potencialmente cubierta. (También cubierto por póliza ciber si el evento es de naturaleza ciber).
- Coste de restauración de programas o sistemas informáticos pertenecientes al asegurado. (cobertura no estándar en *Crime*, habitualmente sujeta a redacción específica o derivada a pólizas Ciber).

Fraude Externo

Actos fraudulentos cometidos por un tercero, actuando solo o en connivencia con un empleado. Incluye robo, falsificación, transferencia fraudulenta de fondos o fraude informático.

Ejemplos:

- Pérdida de fondos mediante la introducción de instrucciones fraudulentas o alteración de los datos en el sistema de información del asegurado mediante una intrusión no autorizada.
- Falsificación de instrumentos de pago.
- Robo de mercancía mediante proveedores falsos.
- Apropiación indebida de activos de terceros bajo la custodia del asegurado.

Dentro de este ámbito cabe destacar el Fraude por Ingeniería Social, dada su proliferación en los últimos tiempos.
Dependiendo del *wording*, las pólizas pueden incluir:

- La pérdida directa sufrida por el asegurado (fondos propios), siendo crítico analizar la definición de pérdida.

- Robo de propiedades o bienes del asegurado perpetrado por un tercero, incluido dinero o valores en tránsito con posible exclusión de determinadas tipologías (ej. desaparición inexplicada, fraude sin acto ilícito probado).
- Robo de bienes de clientes bajo custodia del asegurado cometido por un tercero.
- Gastos y honorarios razonables de los profesionales encargados de investigar las circunstancias de pérdida cubierta o potencialmente cubierta.
- Coste de restaurar los programas o sistemas informáticos pertenecientes al asegurado.

(En los últimos dos casos, también cubiertos por la póliza ciber cuando corresponda).

6.3. Coberturas básicas

Las coberturas esenciales del seguro *Crime* pueden incluir dependiendo del *wording* y del alcance contratado:

- Infidelidad de empleados
  - Apropiación indebida (dinero, valores, datos, ...)
  - Hurto, robo y estafa
  - Falsificación, falsificación de instrumentos de pago...
  - Transferencias fraudulentas
  - Fraude de tarjeta de crédito
  - Infidelidad de empleados desplazados o trabajando en cliente.
- Acto fraudulento de terceros.
- Fraude informático.
- Fraude en transferencias electrónicas.
- Ingeniería social / suplantación de identidad (habitualmentemediante extensión específica y con condiciones estrictas).
- Falsificación y alteración electrónica.
- Uso fraudulento de accesos privilegiados.
- Fraude externo digital.
- Extensión a gastos de investigación / auditoría forense (normalmente sujetas a sublímites y aprobación del asegurador).

La denominación de las coberturas no garantiza su inclusión automática, siendo imprescindible analizar su definición exacta y condiciones de aplicación en la póliza.

6.4. Otras coberturas

Estas coberturas no son estándar de mercado y, por lo general, requieren negociación expresa y aceptación por parte del asegurador. Su alcance, sublímites y condiciones varían significativamente.

Además de las garantías principales, existen otras coberturas que pueden ampliar el alcance de la póliza y permiten adaptar la protección a las particularidades de cada empresa, como por ejemplo:

- Fraude mediante *deepfakes* o IA
- Fraude de proveedores / contratistas externos
  - Cubre pérdidas derivadas de actos fraudulentos cometidos por proveedores de servicios o contratistas con acceso autorizado a sistemas o fondos.
  - Muy útil cuando la externalización de IT/finanzas es significativa.
- Fraude mediante tarjetas o medios de pago electrónicos
  - Cubre pérdidas por uso fraudulento de tarjetas corporativas, pagos electrónicos o *wallets* digitales.
  - Normalmente con sublímites y condicionado a controles de conciliación.
- Cobertura para "Fondos de clientes en custodia" (habitualmente condicionada a requisitos de control interno y segregación de cuentas)
  - Protege frente a pérdidas sufridas por clientes cuando los fondos bajo custodia de la empresa son desviados por fraude interno.
  - Muy relevante en sectores financieros, agencias de viajes, inmobiliarias.
- Pérdida por robo de identidad digital corporativa
  - Cubre pérdidas directas cuando un tercero utiliza la identidad digital de la empresa para cometer fraude económico.
  - No es estándar, se suele pedir como extensión negociada.
- Fraude por cheque electrónico o pago remoto
  - Aunque cada vez menos común, algunos wordings todavía ofrecen coberturas específicas para falsificación de cheques, incluidos en su versión electrónica.

- Deshonestidad de terceros requiere extensión expresa y definición clara de “tercero cubierto”
    - Extensión para cubrir actos cometidos por consultores, becarios, *outsourcing,* que no son empleados en nómina, pero sí actúan bajo la autoridad del asegurado.
- Gastos legales y costes de recuperación
    - Ampliación para cubrir costes de asesoría legal, demandas contra empleados defraudadores, o costes de recuperación de activos robados.
- Fraude en criptoactivos o activos digitales específicos (limitado y sujeto a requisitos estrictos)
    - Algunas aseguradoras empiezan a ofrecer coberturas específicas para cripto / *wallets* digitales, aunque suelen requerir controles de custodia reforzados.
    - Generalmente solo en mercados internacionales o en programas multinacionales.

6.5. Exclusiones

Las exclusiones varían significativamente entre aseguradoras y *wordings*, por lo que el listado siguiente tiene carácter meramente orientativo. Su interpretación concreta dependerá de la redacción de la póliza.

Las pólizas *Crime* establecen una serie de exclusiones que precisan los límites del seguro y delimitan los supuestos que no quedarían amparados. Algunos ejemplos son:

- Pérdida de un asegurado en beneficio de otro asegurado.
- Propiedad Intelectual y secretos comerciales.
- Actos fraudulentos o intencionados cometidos por administradores, socios o accionistas.
- Impuestos, multas y sanciones.
- Pérdida indirecta o consecuenciales (salvo inclusión expresa, poco habitual en este ramo).
- Conocimiento previo de robos cometidos por el mismo empleado.
- Beneficio o pérdida de inventario cuya causa no se puede justificar
- Extorsión o secuestro.
- Cesión Voluntaria.
- Guera y terrorismo.
- Hechos conocidos o descubiertos antes del comienzo de la póliza

- Pérdidas indirectas
- Lucro cesante, pérdida de reputación, daño de imagen.
- Costes de oportunidad o retrasos en proyectos.
- Riesgos de crédito.
- Ciertas exclusiones técnicas, como puede ser el fallo de sistema no causado por acto delictivo, o errores/omisiones contractuales (depende de la redacción).
- Fraudes vinculados a criptomonedas, salvo cobertura específica.
- Pérdidas por incumplimiento de procedimientos contractuales (errores de gestión, E&O) salvo que pueda demostrarse como acto delictivo.
- Incumplimiento de controles declarados o exigidos por la aseguradora, que puede dar lugar a reducción o denegación del siniestro en función de cómo esté recogido contractualmente (condición de cobertura vs. obligación de garantía).

6.6. Ventajas estratégicas del seguro *Crime*

Además de cubrir las pérdidas por fraude interno y externo mencionadas, el seguro *Crime* aporta valor en varias dimensiones clave para *Compliance*, la reputación corporativa y la gestión de riesgos, entre las que destacan:

1 **Fortalecimiento de la cultura ética**

La existencia del seguro refuerza el mensaje de que la empresa toma en serio la prevención del fraude. Esto puede tener un efecto disuasorio interno y fomentar comportamientos éticos, especialmente si se comunica como parte del sistema de control.

2 **Mejora de la trazabilidad y control interno**

La contratación del seguro suele requerir una revisión exhaustiva de procesos, lo que puede impulsar mejoras en trazabilidad, documentación y control de operaciones sensibles (pagos, compras, relaciones con terceros).

3 **Protección reputacional**

Ante un incidente, contar con un seguro permite reaccionar con rapidez y demostrar que la empresa tenía medidas preventivas activas. Esto puede mitigar el impacto reputacional frente a clientes, socios e inversores.

4 **Cobertura de riesgos emergentes**

El seguro *Crime* ofrece una protección adicional frente a escenarios de fraude que, por su novedad o baja frecuencia histórica, no han sido identificados en los mapas de riesgos. Esta cobertura actúa como un mecanismo de defensa ante la evolución de las técnicas empleadas por potenciales defraudadores, permitiendo a la organización anticiparse a vulnerabilidades que aún no han sido formalmente modelizadas o documentadas.

5 **Ventaja competitiva**

Contar con un sistema robusto de prevención y cobertura frente al fraude puede ser un diferenciador frente a competidores que no lo tienen.

6 **Herramienta de negociación con el banco**

Tener un seguro de *Crime* con coberturas de fraude de transferencias puede mejorar la relación con bancos y, en algunos casos, la negociación de líneas de crédito, porque se demuestra protección frente a desfalcos.

6.7. Tendencias del seguro

Las principales tendencias del seguro de *Crime* en el mercado actual son las siguientes:

1 **Franquicia**

La franquicia asumida en este tipo de seguro depende en gran medida del tamaño de la empresa y del límite a contratar. Para una gran empresa se podría esperar un nivel de franquicia no inferior a los 150.000 euros. Empresas menores tendrán interés en franquicias menores. El mercado ya está planteando franquicias en el entorno de 100.000 €.

2 **Límite**

Los límites y franquicias dependen de la estructura del programa, la capacidad disponible y la negociación concreta, no existiendo referencias estándar aplicables a todos los casos.

Para grandes empresas se consideran límites orientativos de 10.000.000 €.

3 Prima

La prima del seguro *Crime* varía según el tipo y tamaño de la empresa, el nivel de controles y protocolos internos implantados y el grado de exposición internacional. Las compañías con operaciones en países de mayor riesgo, estructuras más complejas o menores medidas de control suelen asumir una prima más elevada.

4 Proceso de contratación

Las aseguradoras, durante el proceso de suscripción de este tipo de pólizas, evalúan fundamentalmente los controles internos de los que dispone una organización.
Las medidas de defensa o mitigación interna que se evalúan podrían resumirse en las siguientes:

- ANÁLISIS DE RIESGOS
- POLÍTICAS Y PROCEDIMIENTOS
- PLAN DIRECTOR DE SEGURIDAD
- ÁREAS DE CONTROL DIFERENCIADAS
- FORMACIÓN Y CONCIENCIACIÓN
- PROCESO DE MEJORA CONTÍNUA
- DISGREGACIÓN DE FUNCIONES
- CONTROLES REGULARES POR ÁREAS INDEPENDIENTES
- DETECCIÓN Y VULNERABILIDADES
- CORTAFUEGOS Y ANTIMALWARE
- PÓLIZAS CRIME Y CIBER

La evaluación de estos controles suele realizarse mediante formularios que el asegurado debe completar, en los que se recogen los procedimientos, medidas de seguridad y controles internos implementados. La información facilitada en dichos formularios es asumida por la compañía aseguradora como prueba de la existencia y aplicación efectiva de los controles declarados.

La falta de existencia real de esos controles o su no aplicación práctica, pese a haber sido informados en el cuestionario, puede derivar en la no cobertura de un siniestro, al considerarse que el riesgo presentado no coincide con el riesgo realmente asegurado.

Por ello, es imprescindible que este enfoque esté correctamente reflejado en el redactado de la póliza, donde deben detallarse las circunstancias en las que la aseguradora podría excluir la cobertura por incumplimiento de controles declarados. Resulta, por tanto, fundamental revisar el redactado con detalle, a fin de identificar con precisión qué eventos están cubiertos y en qué situaciones la compañía podría limitar o excluir su responsabilidad.

En resumen, las aseguradoras basan su suscripción en los controles declarados, que en muchos casos se incorporan como base del contrato, pudiendo impactar directamente en la cobertura.

La veracidad y aplicación efectiva de los controles declarados son un elemento esencial, ya que discrepancias entre lo declarado y la realidad pueden derivar en controversias o en la limitación de cobertura.

6.8. Tendencias del mercado

Las principales tendencias del mercado asegurador reflejan:

1 **Evolución**

La capacidad del ramo de *Crime*, tanto en el mercado español como en el internacional, ha experimentado importantes fluctuaciones a lo largo de la última década. Se trata de un ramo con escasa penetración en el mercado nacional, lo que se traduce en un volumen de primas reducido. Esta circunstancia, unida a que la siniestralidad suele ser elevada —dado que las empresas que contratan este tipo de seguro son, habitualmente, las más expuestas a riesgos de fraude— convierte al ramo en una línea de negocio altamente tensionada.

Como consecuencia, existe poca capacidad disponible en el mercado y, sobre todo, un número limitado de aseguradoras dispuestas a suscribir este tipo de riesgos.

Sin embargo, en el periodo postpandemia, la tendencia de mercado "blando" existente en general en todas las líneas financieras (familia en la que se engloba el seguro *Crime*), con un aumento de la capacidad disponible y ajuste en los precios, se ha trasladado al mundo *Crime*.

También se aprecia una mayor rigurosidad en la suscripción del riesgo, así como un aumento de la penetración del seguro, esto último muy ligado a los casos de fraude por Ingeniería Social, sobre todo al conocido como "Fraude del CEO".

2 **Capacidad**

La capacidad, aunque ha aumentado, sigue restringida a un número reducido de aseguradores. La máxima capacidad que suelen exponer estos mercados oscila entre 5 y 7,5 millones de euros, por lo que, si se quiere contratar un límite superior, es necesario recurrir a coaseguros o colocaciones tipo torre. La estructura más efectiva suele ser la torre, ya que el número de compañías dispuestas a aportar capacidad aumenta de manera significativa cuando existe un asegurador primario

y facilita alcanzar límites más elevados de manera ordenada y estable, aumentando la competencia.

Los "players" principales a la hora de contratar un primario son Liberty, Zurich, QBE, AIG, Sompo, Allianz, Euler y AXA XL.

Otros mercados que podrían aportar capacidad sobre todo en excesos son ANV, Beazley, Berkshire Hathaway, Chubb, Everest y Tokio Marine HCC.

Se estima que en el mercado español existen unos 80.000.000 euros de capacidad que podrían llegar hasta los 300.000.000 euros considerando todo el mercado mundial.

6.9. Diferencias del seguro *Crime* vs Ciber

Aunque el seguro ciber y el seguro *Crime* pueden relacionarse con riesgos digitales, responden a exposiciones distintas. El seguro ciber protege a la empresa frente a las consecuencias de un incidente tecnológico externo, mientras que el seguro *Crime* se centra en el fraude y la deshonestidad, tanto internas como externas, que generan pérdidas económicas directas.

Ambos productos no se solapan, sino que se complementan para proporcionar una protección integral frente a los riesgos digitales y financieros actuales.

Las principales diferencias son:

1 **Naturaleza del riesgo cubierto**

- Seguro ciber: se centra en incidentes derivados de ataques externos al sistema (pérdida de datos, ransomware, brechas de seguridad, interrupción del negocio, sanciones regulatorias por RGPD, etc.).
- Seguro *Crime*: protege frente a pérdidas económicas directas ocasionadas por fraude o deshonestidad, en especial los cometidos por empleados o a través de técnicas de manipulación digital (fraude informático, ingeniería social, transferencias fraudulentas).

2 **Tipo de pérdida indemnizada**

- Seguro ciber: cubre tanto gastos de gestión del incidente (forense, notificación, defensa legal, relaciones públicas) como pérdida de beneficios por interrupción del negocio.
- Seguro *Crime*: cubre sobre todo la pérdida patrimonial directa (dinero, valores, activos) sufrida por la empresa como consecuencia del fraude.

3 **Origen de la amenaza**

- Seguro ciber: principalmente amenazas externas (*hackers*, ciberdelincuentes, *malware*).
- Seguro *Crime*: históricamente internas (empleados), aunque hoy en día también contempla fraude externo mediante suplantación o ingeniería social.

4 **Origen de la amenaza**

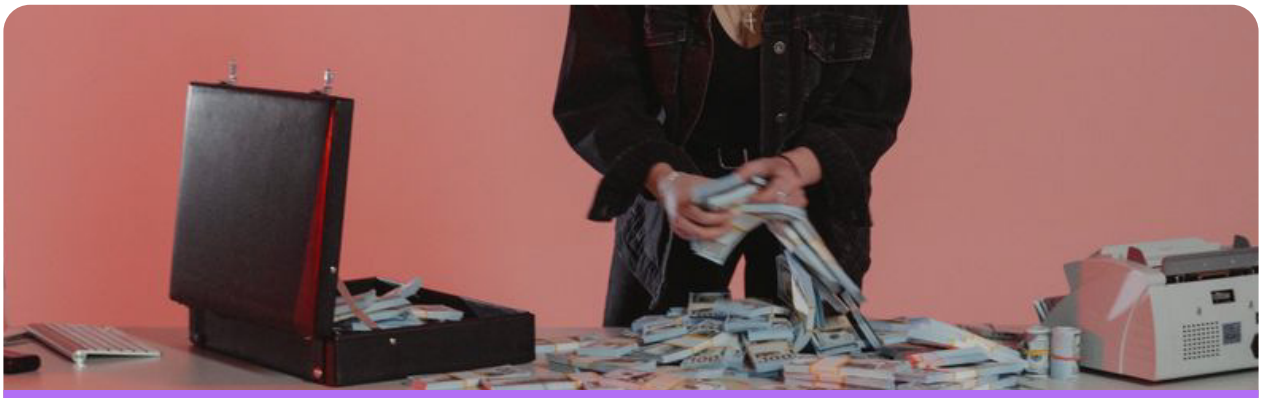
- Seguro ciber: enfoque tecnológico y de gestión de crisis, con paquetes de servicios asociados.
- Seguro *Crime*: enfoque financiero-contable, centrado en la protección de activos frente a fraude.

Existen productos que dan coberturas *Crime* dentro de póliza ciber y otros que dan conjuntamente coberturas de ciber y *Crime*, como criber de HOWDEN.

7. Casos prácticos

Los fraudes analizados en este capítulo ilustran una realidad cada vez más frecuente en las empresas: **el delincuente no necesita vulnerar grandes sistemas técnicos si consigue manipular a las personas y los procesos.** A través de la suplantación de identidades, el uso de canales de comunicación aparentemente legítimos y la explotación de situaciones de urgencia operativa o presión jerárquica, los atacantes logran que sean los propios empleados quienes ejecuten las acciones que generan el daño económico.

Estos casos muestran además una evolución clara del fraude tradicional hacia esquemas **híbridos**, donde confluyen ingeniería social, conocimiento profundo del negocio, accesos no autorizados a sistemas de información y, más recientemente, el uso de herramientas de inteligencia artificial como los deepfakes. El objetivo ya no es solo engañar, sino **hacerlo de forma creíble, coherente con los procedimientos internos y difícil de detectar en tiempo real.**



Desde la perspectiva del responsable de seguros, estos incidentes ponen de manifiesto dos cuestiones clave. En primer lugar, la importancia de **comprender correctamente el alcance y las diferencias entre las coberturas *Crime* y Ciber,** evitando falsas expectativas sobre qué daños están o no amparados. En segundo lugar, la necesidad de que el seguro no sea visto como un sustituto de los controles internos, sino como un **complemento dentro de una estrategia integral de prevención, detección y respuesta al fraude.**

Los siguientes casos ilustran cómo se materializan los distintos tipos de fraude analizados, poniendo de manifiesto la interacción entre factor humano, procesos internos y mecanismos de aseguramiento.

7.1. PAGO A PROVEEDOR

Engaño mediante modificación fraudulenta de cuentas bancarias, manipulación de correos y presión sobre el empleado. Cobertura completa por la póliza Crime tras verificarse la existencia de fraude externo.

La compañía se dedica a la fabricación de componentes auxiliares para el sector de automoción. Un número importante de proveedores se encuentran ubicados en Asia.

Uno de los proveedores de Vietnam llama a su interlocutor (X) para informarle que todavía no han recibido el pago de la última factura, a pesar de que ya se ha superado en 15 días el plazo del pago.

X habla con contabilidad para confirmar la situación del pago y le confirman que este fue realizado en plazo y le adjuntan los justificantes. A continuación, llama a Vietnam y envía por correo los justificantes. Poco después recibe la noticia de que los pagos se han realizado a una cuenta incorrecta.

X recuerda que hace un mes recibió una comunicación de su interlocutor en la empresa vietnamita (Z) para informarle que habían dejado de trabajar con el banco en el que X realizaba los pagos y lo han sustituido por otro. Pocas horas después recibió la comunicación concretando lo hablado por teléfono.

Z informa a X que es cierto que estaban realizando gestiones para cambiar de banco, pero que todavía no lo habían comunicado a ninguno de sus clientes y que no trabajaban ni tenían intención de trabajar con el banco al que habían efectuado el pago. Z le urgía a realizar el pago si no querían que suspendieran el envío de las próximas mercancías. La factura ascendía a 99.527 euros. La empresa trabaja con un nivel muy bajo de stocks, por lo que se pondría en riesgo la continuidad de la producción.

Z aprovecha para indicarle que, como ya le había contado, han empezado a trabajar con un nuevo banco y que por favor, envíen el pago a la nueva cuenta, de la que envía un correo en ese momento.

La compañía ordena una nueva transferencia al proveedor. Como tiene un seguro *Crime*, activa la póliza. También comunica a la policía el fraude del que ha sido objeto.

Una semana después, X vuelve a recibir una llamada de su interlocutor en el proveedor vietnamita, para informarle que a pesar de haber superado en tres semanas el plazo de pago, tienen pendiente una factura de 99.527 euros. X informa al nuevo Z de la conversación mantenida hace 7 días, a lo que Z indica que no se ha puesto en contacto con X en los últimos 6 meses y que no han cambiado de banco.

Las investigaciones realizadas por la policía y la aseguradora confirman que X ha sido engañado. Las direcciones de los correos recibidos (distintos en cada caso) eran muy similares a las del proveedor, pero no iguales.

El dinero enviado fue transferido de forma casi inmediata a otras cuentas sin que haya forma de seguir el rastro final.

La compañía aseguradora confirma la cobertura del seguro por fraude y paga al asegurado los dos siniestros, descontando la franquicia, que se aplica dos veces. El pago se realiza en el plazo de un mes desde la apertura del siniestro. El importe total del siniestro se encuentra por debajo del límite asegurado. La aseguradora exige al asegurado reforzar los procedimientos para realizar los cambios de las cuentas de pagos.

La compañía ha realizado las siguientes acciones: i) incorporar en las acciones de concienciación al personal el caso que han sufrido y ii) establecer como procedimiento para recoger las cuentas corrientes de pago la llamada a interlocutores utilizando registros previos y la autorización de los proveedores para que los bancos confirmen la titularidad de las cuentas.

Los delincuentes habían estado estudiando al fabricante y a sus proveedores, la criticidad de los suministros, las personas responsables de las compras, sus interlocutores con los proveedores, los procedimientos de pago, del cambio de cuentas de pago, el importe habitual de las facturas, etc.

7.2. Fraude en la entrega de mercancía

Intrusión en sistemas y desvío de mercancías de alto valor. Cobertura aplicable solo por *Crime*. Investigación forense y recuperación parcial.

La compañía es un mayorista de productos electrónicos dirigidos a particulares, fundamentalmente televisores, ordenadores, tabletas y telefonía móvil.

Uno de sus principales clientes, una cadena de retail, llama a su vendedor para reclamarle un pedido que todavía no han recibido y que necesitan urgentemente pues faltan pocos días para una campaña que tienen prevista y de la que estiman una alta venta de la mercancía no recibida.

El vendedor habla con logística, que le confirma que el pedido fue entregado hace tres días. La revisión de la entrega pone de manifiesto que el lugar de entrega no era el habitual. Esta se ha realizado en un polígono industrial en donde la empresa de retail no tienen ningún almacén.

Se revisan las comunicaciones mantenidas con la empresa de retail y en ningún caso figura un cambio del lugar de entrega habitual. Pero en el sistema de información figura el lugar en el que se ha realizado la entrega incorrecta.

Se da intervención al área de sistemas de información para averiguar el usuario que ha realizado el cambio. El que figura es el que realizó el cambio hace un año, cuando se realizaban las entregas en el almacén principal del cliente.

Los primeros pasos de la investigación establecen como hipótesis más probable que se haya producido un acceso no autorizado en los sistemas de información de la compañía y se han alterado las direcciones de envío. Se da intervención al CISO de la empresa.

La compañía tiene contratada una póliza Ciber y otra *Crime*, que activan. Se informa también a la policía.

La aseguradora de la póliza ciber rechaza la cobertura, al ser el objeto del daño mercancía. La póliza solo habría cubierto el daño si se hubiese producido como consecuencia del acceso no autorizado, un movimiento de fondos.

La póliza *Crime* tiene cobertura para esta situación. Un equipo forense suministrado por la aseguradora analiza con la colaboración de la empresa como se puede haber producido el incidente.

La empresa llama a todos los clientes a los que ha enviado mercancía recientemente para conocer si los han recibido de forma correcta. Al resto pide confirmación del lugar de envío. Esta acción pone de manifiesto que el caso reportado no es un caso aislado; existen otros cinco casos más y todos los envíos superan los 100.000 euros. En algunos casos la mercancía tenía un destino erróneo que se corrige antes de la entrega.

La urgencia en recibir la mercancía del proveedor que tenía la campaña prevista limitó la dimensión del fraude que alcanza casi un millón de euros.

La nave en la que se había realizado la entrega era una nave que se encontraba desalquilada en un polígono con poca actividad. Los vecinos detectaron actividad puntual hace unos días, en los que se abrió, limpió y colocaron unos carteles que luego fueron retirados.

Siguiendo las instrucciones de la policía, uno de los pedidos se entrega en la dirección falsa. La policía detiene a las personas que recogen la mercancía, pero estos eran meros intermediarios que recogían la mercancía trasladándola de un camión a otro de un tercero desconocido en un

punto acordado por teléfono. No se consigue determinar quién era ese tercero.

El análisis forense confirma la intrusión no autorizada. La compañía incorporará las recomendaciones de los forenses para prevenir en un futuro ataques similares.

La aseguradora se hace cargo de todos los gastos forenses y el importe de la mercancía defraudada, descontando una vez la franquicia (al tratarse de un único siniestro).

No es posible entregar al cliente que iba a realizar la campaña toda la mercancía prevista en el corto plazo por no tener suficientes existencias. El cliente solicita una compensación asociada a la pérdida de beneficios por la venta que va a perder. Aunque contractualmente la compañía no tiene esta obligación, para mantener la buena relación con el cliente, acuerda una compensación a través de la rebaja del precio de la mercancía que aplicará durante los próximos tres meses. Esta cantidad no está cubierta por el seguro.

7.3. Fraudes del CEO

Deepfakes y suplantación de órganos de gobierno. Transferencias realizadas por un CFO engañado. Cobertura *Crime* y establecimiento posterior de protocolos de proyectos confidenciales.

La compañía es una empresa de tecnología multinacional con sucursales en distintos países. Está creciendo de forma importante, siendo parte fundamental de su estrategia la compra de sociedades incipientes que están destacando en el desarrollo de la IA.

Su oficina principal está en Alemania y la estructura que tienen en otros países es relativamente pequeña. Aunque en España tienen un Director General, la dependencia funcional de los distintos directivos es con Alemania.

El CFO de España (X) se considera una persona con un gran potencial y está empezando a pensar que su puesto se le está quedando pequeño. Aspira a ser trasladado a la oficina de Alemania.

El CEO de la empresa es considerado uno de los grandes visionarios de la IA. Es una persona de trato difícil, muy autoritaria y que no admite errores.

X recibe un día una llamada del PA del CEO para informarle que va a ser invitado a participar en un Grupo de Trabajo que tiene como objetivo comprar otra empresa tecnológica, además de informarle que el CFO mundial está muy satisfecho de su trabajo y ha pensado en él para este proyecto. La empresa que se quiere comprar, muy conocida dentro del mundo especializado, ha desarrollado una nueva tecnología que supondrá una ventaja competitiva importante para la empresa que la incorpore. La participación requiere máxima confidencialidad, por lo que debe firmar un contrato de confidencialidad que le envían por correo.

El Grupo de trabajo lo componen los directores mundiales de tecnología, legal y financiero, además de los CFO de España y Francia.

La relación que ha tenido X con el resto de componentes del Grupo de Trabajo es casi inexistente, con la excepción de CFO mundial, con el que ha tenido varias reuniones telemáticas junto con los CFO de otros países. Del resto de las personas conoce las fotografías que figuran en el organigrama de la organización.

El Grupo de Trabajo va a mantener reuniones de forma telemática. En la primera reunión

participa al comienzo el CEO, que incide en la importancia de que la compra se lleve a cabo y de la más absoluta confidencialidad. Para reforzar esta, se han creado unos usuarios de correo específicos para esta operación. Las conversaciones deben limitarse a las que se mantengan en las distintas reuniones.

A los directores financieros se les solicita que vayan realizando pagos para proceder a la compra de la sociedad. Cuando ésta se complete y se haga pública la operación, que además se estima producirá un aumento del valor de las acciones, se regularizará la situación contable.

El primer pago que se debe realizar desde España es de 250.000 euros. Más adelante, una vez realizado éste, se solicita otro pago de 1 millón de euros. Cuando solicitan el tercero, X informa que no dispone de tesorería para pagarlo. En la reunión, el CFO mundial indica que aporte lo que pueda (otros 250.000 euros) y que el resto lo añadirán a lo que debe aportar Alemania y Francia.

Tras esta reunión, X no vuelve a ser convocado ni recibe noticias ni respuestas en los correos creados para esta operación. Pasan los días y acaba dirigiéndose por la vía convencional al CFO mundial, que le informa que la empresa no está en un proceso de compra de esa sociedad, ni X está en ningún grupo de trabajo confidencial.

Se notifica la situación al Director de Seguridad mundial para que investigue lo ocurrido. La compañía tiene una póliza Crime que se activa.

Los criminales estuvieron estudiando, dedicando especial atención a las redes sociales, empresas que estuvieran participando en la compra de forma confidencial de sociedades, CFOs con autoridad para realizar transferencias de altos importes, con egos y ambiciones elevadas, con poca relación directa con sus superiores, además de una dirección general muy autoritaria y exigente. En las reuniones mantenidas de forma telemática, excepto X el resto eran personajes creados con IA.

El fraude también se comunica a la policía.

La póliza cubre el incidente y paga la cantidad defraudada a la compañía, descontando la franquicia. Se produce una investigación y en menos de un mes se realiza el pago.

La compañía crea un protocolo para proyectos confidenciales que es distribuido entre la Dirección para evitar que se repitan situaciones como ésta.

8. Conclusiones del grupo de trabajo

El análisis realizado por el Grupo de Trabajo confirma que el fraude cibernético, y en particular el basado en ingeniería social avanzada, constituye **uno de los riesgos más relevantes, dinámicos y complejos** dentro del perímetro de los seguros *Crime*. Los siniestros analizados confirman que no se trata de incidentes aislados o excepcionales, sino de **escenarios recurrentes**, altamente adaptados a los procesos, personas y estructuras de cada organización.

De forma resumida, el análisis realizado confirma que:

1 **La ingeniería social es el principal vector de fraude**, tanto por frecuencia como por severidad potencial. Su creciente sofisticación —incluyendo *business email compromise* (BEC), *social engineering fraud* (SEF) multicanal y *deepfakes*— exige controles sólidos, pero también **procedimientos realistas**, compatibles con la operativa diaria y la presión del negocio.

2 **La gobernanza de la identidad y de la autoridad** —incluyendo la gestión de accesos, la validación de interlocutores y el control del uso de IA generativa— se ha convertido en un **componente estructural del riesgo corporativo**, con impacto directo en el diseño y la activación de las coberturas.

3 **La calidad y trazabilidad de los controles internos influyen de manera directa y creciente** en la suscripción: primas, franquicias, sublímites, exclusiones y *wording*. No basta su existencia formal: **es clave su aplicación efectiva y capacidad de acreditación** en caso de siniestro.

4 **Los ataques actuales combinan múltiples técnicas y canales** (correo, mensajería, voz, vídeo, accesos no autorizados, manipulación de procesos), apoyándose habitualmente en **fallos de segregación de funciones, conciliación o escalado**. En consecuencia, la defensa no puede ser puntual ni reactiva, sino **integral y coordinada**.

5 **Las pólizas de Crime y Ciber deben funcionar como programas complementarios**, no como compartimentos estancos. La ausencia de una interfaz clara entre ambas genera zonas grises, conflictos de interpretación y retrasos en la respuesta aseguradora en momentos críticos.

Implicaciones prácticas para una cobertura efectiva

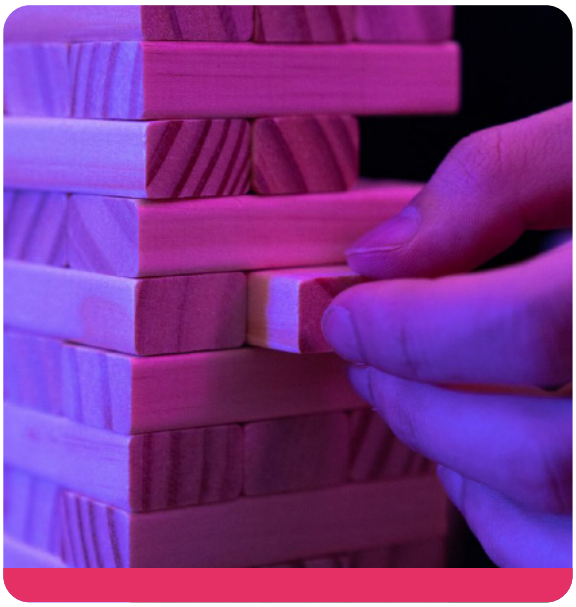
De las conclusiones anteriores se desprende que la **transferencia eficaz del riesgo de fraude** no es un mecanismo exclusivamente asegurador, sino que requiere una **corresponsabilidad activa del asegurado**. La efectividad real de la cobertura depende, en gran medida, del grado de madurez del sistema de control interno y de su adecuada alineación con las exigencias del mercado asegurador.

En este sentido, resulta imprescindible adoptar un **enfoque sistemático, preventivo y dinámico**, basado en la revisión periódica del mapa de riesgos, con especial atención a los procesos, operaciones y flujos expuestos a escenarios de fraude cada vez más sofisticados. Asimismo, es **crítico poder acreditar la implantación efectiva de controles mediante evidencias documentales**.

La experiencia del mercado confirma que los controles internos son un factor determinante en la fijación de primas, franquicias, sublímites y capacidad. En particular, las aseguradoras están intensificando su foco en los controles vinculados a la autorización y verificación de pagos, los procesos de conciliación, la adecuada segregación de funciones, la trazabilidad de las instrucciones recibidas y ejecutadas, así como en los marcos de gobernanza asociados al uso de tecnologías emergentes, incluida la inteligencia artificial. La mera declaración de controles, sin evidencias de su uso efectivo, resulta insuficiente.

La ausencia de controles adecuados, o su aplicación deficiente, puede comprometer directamente la cobertura. Por ello, se recomienda reforzar programas de **formación específica en riesgos de fraude BEC, suplantación avanzada y *deepfakes***, establecer procedimientos claros de escalado en función del importe o la criticidad de las operaciones, y estructurar sublímites y capacidades alineadas con la exposición real, evitando soluciones estándar que no absorben siniestros de impacto relevante.

Resulta esencial analizar en **la cobertura de ingeniería social**, especialmente los requisitos de verificación (incluidas las cláusulas de *call-back*) y las exclusiones por incumplimiento de controles.



Se recomienda revisar y renegociar exclusiones críticas —especialmente las relativas a cesión voluntaria e incumplimiento de controles— evitando estándares de "cumplimiento perfecto" y promoviendo criterios razonables basados en controles esenciales (doble validación, *call-back*, segregación de funciones).

En paralelo, se recomienda **actualizar los *wordings*** para reflejar las tipologías actuales de fraude (incluyendo *deepfakes* y canales multiformato) y emplear definiciones funcionales que reduzcan controversias interpretativas.

Adicionalmente, resulta aconsejable analizar cláusulas relativas al conocimiento previo, pérdidas indirectas y exclusiones técnicas, e incorporar, cuando proceda, coberturas complementarias como la custodia de fondos de clientes o, de forma muy controlada, coberturas relativas a criptoactivos, siempre acompañadas de controles reforzados.

Finalmente, la **coordinación entre las pólizas de *Crime* y Ciber** emerge como un elemento crítico para evitar solapamientos, vacíos de cobertura y conflictos en la gestión del siniestro. La definición clara de la interfaz entre ambas pólizas, la adecuada prelación de coberturas y, cuando sea posible, la contratación conjunta de ambas coberturas con una misma aseguradora contribuye de manera significativa a una respuesta más eficiente y predecible.

Desde una perspectiva de mercado, la **capacidad disponible en el tramo primario continúa siendo limitada**. En este contexto, la estructuración de programas en capas —combinando póliza primaria y excesos— se consolida como una herramienta eficaz para ampliar límites, optimizar costes y mejorar la competitividad, sin deteriorar las condiciones de activación de la cobertura.

En síntesis, la gestión del fraude no se limita únicamente a la compra de capacidad, sino en la **alineación entre controles operativos, gobernanza, diseño del programa y negociación**

contractual. El Grupo constata divergencias significativas en definiciones y coberturas, lo que refuerza la necesidad de un papel activo del asegurado.

Finalmente, los siniestros más complejos no derivan únicamente del engaño inicial, sino de la **combinación de técnicas avanzadas, multiplicidad de canales y debilidades en los procesos internos**. Integrar estos elementos en la gestión del riesgo es una **condición necesaria para la resiliencia financiera y operativa de las organizaciones.**

La correcta gestión del fraude en el entorno cibernético exige una visión integrada que combine gobernanza, controles operativos y diseño asegurador. Esta guía pretende servir como referencia práctica para avanzar en esa dirección.

9. Sobre la comisión de riesgos tecnológicos de Agers

Breve presentación de la comisión y enlaces a publicaciones anteriores.

1. **Casos Prácticos de Siniestros Cibernéticos y su gestión y participación del Seguro. Año de publicación: 2024.**
2. **Buenas prácticas en protección de Ciberriesgos para no expertos. Año de publicación: 2023.**
3. **Estudio Pólizas de Ciber del Mercado Español. Año de publicación: 2020**
4. **Mapa de Ciberriesgos. Año de publicación: 2019.**
5. **Top 10 Ciber Risks. Año de publicación: 2018.**
6. **GUÍA DE TERMINOLOGÍA DE CIBERSEGURIDAD. Año de publicación: 2017.**

10. Entidades colaboradoras

Esta guía, elaborada por la Comisión Ciber de AGERS, tiene un enfoque técnico y práctico, y está dirigida a profesionales de la gestión de riesgos, finanzas, compliance, seguridad de la información y seguros. Su objetivo es analizar el fraude en el entorno cibernético desde una perspectiva operativa y aseguradora, aportando criterios de entendimiento, prevención y adecuada transferencia del riesgo.

El fraude en el entorno cibernético

Asociación española de gestión de riesgos y seguros AGERS

ISBN: 978-84-09-88323-3

Copyright: DEP639172022768438887