

De los criptoactivos al Compliance

Prevención de riesgos legales
en la economía digital

Marcos Romero Perin

Trabajo Integrador Final

Curso Superior en Derecho, Economía Digital y CriptoActivos
Universidad de Salamanca - España

Marcos Romero Perin

MRP | LegalTech
www.marcosromeroperin.com
linkedin.com/in/marcosromeroperin

Publicación web y descarga
Archivo académico profesional

Referencia académica

Trabajo Integrador Final

Curso Superior en Derecho, Economía Digital y CriptoActivos
Universidad de Salamanca - España

Trabajo presentado y finalizado en enero de 2024
Publicado originalmente en LinkedIn
31 de enero de 2024



Reconocimiento académico

TIF que ha obtenido una Mención Especial por parte del Director del Curso de Especialización, Profesor Dr. Ignacio Leo Castela: **Sobresaliente**

«El trabajo de este estudiante sobresa de lo común. En primer lugar, la temática escogida resulta vanguardista, original y muy pertinente. El abordaje que realiza el alumno es valiente por cuanto aborda cuestiones jurídicas complejas y, sin embargo, las sabe exponer con acierto aportando reflexiones personales y opiniones críticas que enriquecen mucho el discurso. La bibliografía consultada es amplísima y rigurosa. El lenguaje es correcto y atractivo y las conclusiones que arroja este alumno demuestran un alto grado de conocimiento sobre esta materia. En definitiva, sobran razones para considerar que el alumno ha superado este curso superior de especialización de manera sobresaliente.»

Fdo.: Prof. Juan Ignacio Leo Castela - DIRECTOR

Nota editorial

El documento conserva su formulación original. Algunas referencias regulatorias deben leerse en el contexto temporal de su elaboración y publicación original.

Índice

Ruta de lectura editorial

Índice

1. Introducción	3
2. Desarrollo	3
2.1. Las criptomonedas	3
2.2. El delito de moda con el surgimiento de los criptoactivos	5
2.3. Estafa, esquema Ponzi y sistema piramidal	6
3. Responsabilidad penal de las personas jurídicas y doble vía de imputación	8
3.1. Catálogo de delitos	9
3.2. Penas que pueden imponerse a personas jurídicas	10
3.3. Responsabilidad civil directa y solidaria de la persona jurídica	10
3.4. Circunstancias modificativas de la responsabilidad penal	10
4. Qué es el Compliance y su necesidad	12
4.1. La importancia y necesidad de Compliance en las organizaciones	13
4.2. Qué es un programa de cumplimiento normativo	14
4.3. Cumplimiento normativo y cumplimiento penal	17
4.4. Ventajas de proponer un Compliance penal	20
4.5. Norma ISO 37301 sobre sistemas de gestión de Compliance	20
5. Primer intento serio de regulación europea: Reglamento MiCA	21
6. Casos de interés	22
6.1. Caso Hans J. Neubürger (Siemens)	22
6.2. Casos de interés involucrados con criptomonedas	22
6.3. El boom de las macroestafas de criptos ante la Audiencia Nacional	23
7. Conclusiones	23
8. Recursos bibliográficos	25
8.1. Bibliografía básica	25
8.2. Bibliografía complementaria	25
8.3. Otros recursos	26

1 Introducción

El Presente trabajo tiene el objetivo de dar un breve panorama de la situación actual referente a la implementación de las criptomonedas como sistema descentralizado de intercambio de activos mediante el cual, miles de personas descubrieron que las monedas digitales les ofrecen un sistema financiero alternativo, transparente, abierto y sin trabas. Pero los cibercriminales están al acecho, pareciera que informarse sobre las características de los proyectos e invertir a conciencia no es el único arma para defenderse, sino también, es necesario desarrollar una legislación específica sobre el tema que de una protección a los usuarios y consumidores. Y uno de esos caminos, y el cual cada día se ve con más claridad, lo podríamos denominar como el camino del Compliance y la prevención de riesgos legales.

El análisis y desarrollo de los puntos que a continuación expondré, están basado inicialmente en mi experiencia como consumidor y usuario de criptoactivos, como abogado penalista de varios años de profesión y en mis estudios académicos realizados en el Reino de España en los últimos 15 años. Cuya Legislación sigo exhaustivamente, por considerarla avanzada en algunos aspectos técnicos penales y enmarcada por la jurisprudencia juntamente también con las directivas de la Comunidad Europea (CE).

Con lo expuesto anteriormente quiero advertir al lector, que la base para el análisis, por ejemplo, de la Responsabilidad de las Personas Jurídica (RPJ), es en base al Código Penal español reformado en el 2015, como así también los casos prácticos que citó como ejemplo sobre estafas con criptomonedas y en lo referente al Corporate Compliance, cuya Maestría he finalizado muy recientemente.

2 Desarrollo

2.1 Las criptomonedas

Una criptomoneda es un activo digital que emplea un cifrado criptográfico para garantizar su titularidad y asegurar la integridad de las transacciones, y controlar la creación de unidades adicionales, es decir, evitar que alguien pueda hacer copias como haríamos, por ejemplo, con una foto. Estas monedas no existen de forma física: se almacenan en una cartera digital. (Guia Santander, 2022)

Entonces, podríamos definir las criptomonedas, criptodivisas o criptoactivos, como un activo digital de intercambio, que no existen de forma física, sino que se almacenan en una cartera digital. A las criptomonedas se les emplea un cifrado que garantiza su titularidad, la integridad de las transacciones, así como evitar que se hagan copias. Se trata de activos descentralizados, puesto que no son controladas por un único servicio o empresa, como sí pasa con las monedas

convencionales, organizadas por entidades y bancos. (Conf. Definición dada por el tutor Manuel Lopez, Módulo 2, Curso Criptoactivos 2022).

El auge de las criptomonedas, como el bitcoin, ha provocado un cambio en la forma de ver la economía, las finanzas y, también, la ciberseguridad. Ha sido realmente, una revolución que muchos la comparan con la creación e implementación de Internet.

Bien claro ha sido el informe Especial del Banco de España de Criptoactivos (primavera 2022), cuando dice que: "La tecnología de criptoactivos está creando nuevos activos financieros y nuevas maneras de intermediación. Las tecnologías que lo sustentan pueden potencialmente mejorar la eficiencia y la resistencia del sistema financiero bien a través de unos menores costes en las transacciones, una mayor interoperabilidad en el sistema de pagos o de una mayor competencia entre los distintos actores. Ahora bien, esos beneficios sólo se podrán obtener si su desarrollo se efectúa de manera segura y viene acompañado de marcos regulatorios que mitiguen los riesgos y mantengan la confianza en el sistema financiero".

Como toda implementación de algo nuevo, posee ventajas y desventajas (riesgos) que se deberían mitigar mediante el uso y desarrollo de esta nueva tecnología descentralizada, pero que en algunos casos también es centralizada, como por ejemplo es el caso de los Exchange criptos.

Por ejemplo, refiriéndonos a los Exchange y comparándolos con los Bancos Tradicionales, podemos destacar Tres tipos de riesgos muy bien detallados por el tutor Manuel Lopez (curso Criptoactivos 2022, Salamanca):

El primer riesgo es el de una huida bancaria o como se conoce en España y Argentina, corralito. Una huida es lo que ocurre cuando un grupo de personas se presenta a la vez y quiere recuperar su dinero. Como el banco solo mantiene reservas fraccionarias, podría ser incapaz de hacer frente a las retiradas simultáneas.

El segundo riesgo es que los propietarios de los bancos puedan ser simplemente ladrones que dirigen un esquema Ponzi. Se trata de un esquema en el que alguien consigue que la gente le dé dinero a cambio de beneficios en el futuro, pero luego realmente toma su dinero y lo utiliza para pagar los beneficios a las personas que compraron previamente.

El tercer riesgo es el de un hackeo, el riesgo de que alguien -quizá incluso un empleado del exchange- consiga penetrar en la seguridad del exchange.

Todas estas cosas han ocurrido. Hemos visto exchanges que han fracasado debido al equivalente a un corralito bancario. Hemos visto exchanges que han fracasado debido a que los operadores de la exchanges son unos sinvergüenzas, y hemos visto bolsas que han fracasado debido a robos.

El último caso de una quiebra fraudulenta lo podemos ver a través del caso de unos de los exchange criptos más grandes y que poseían registro en EEUU, estamos hablando de FTX: Tres claves para entender la caída de FTX y sus posibles consecuencias:

<https://www.nytimes.com/es/2022/11/22/espanol/caida-ftx-sam-bankman-fried.html>

Las criptomonedas tienen un nivel de regulación intrínsecamente bajo y no están gobernadas por una autoridad central, lo que significa que las transacciones no pueden ser supervisadas de cerca. Esto las convierte en un refugio para la actividad delictiva en todo el mundo, pero a la vez, debemos reconocer que ha traído un cambio increíblemente enorme desde el punto de la seguridad en las transacciones, desarrollo tecnológico e implementación de la tecnología a las finanzas tanto descentralizadas como centralizadas.

La cuestión central, y en donde se deberá trabajar con objetividad, es en lograr una seguridad a fin de proteger a los usuarios, consumidores e inversores criptos. Y esta tarea, desde mi humilde opinión, quedará principalmente en manos de los Estados y entidades privadas debidamente controladas por una legislación precisa y acorde a estas necesidades.

2.2 El delito de moda con el surgimiento de los criptoactivos

El delito más conocido de todas las décadas, desde mi opinión, ha sido el delito de Estafa. Más allá de las particularidades de cada tipo de estafa, en el derecho comparado podemos encontrar notas características de este delito que han sido muy bien definidas por el Tutor Leo Castela (2022):

- la existencia de ánimo de lucro,
- el uso de engaño suficiente o bastante,
- la intención de generar o de inducir a un error,
- la realización de un traspaso patrimonial en perjuicio de un tercero,
- la existencia de un nexo causal entre el engaño causado y el perjuicio económico.

Este delito ha tenido un gran auge en tiempos remotos, volviendo nuevamente a ponerse de moda, con el surgimiento de las criptomonedas. Aparecieron miles de plataformas que ofrecen altos rendimientos por depositar los activos en ellas, y en un corto plazo, simulan presentar problemas, quedándose con los fondos de todos los inversionistas.

Casos de renombre que han sido de resonancia en los medios de comunicación y que han captados miles y miles de millones de dólares de los inversionistas que creían hacerse ricos en poco tiempo, podemos nombrar los siguientes entre muchas otras:

Liberty Reserve; One Coin; Arbistar; Kuallian; Mind Capital; Nimbus; Ganancias Deportivas; FTX

2.3 Estafa, esquema Ponzi y sistema piramidal

Más allá de todas las definiciones que podamos encontrar, comparto el concepto desarrollado en el diccionario de economía publicado en el economista.es (2022), que define un esquema Ponzi como: “una forma de estafa piramidal que atrae a los inversores y paga utilidades a los inversores anteriores con fondos de inversores más recientes. Este esquema lleva a las víctimas a creer que las ganancias provienen de actividades comerciales legítimas (por ejemplo, ventas de productos y/o inversiones exitosas), y desconocen que otros inversores son la fuente de los fondos. Un esquema Ponzi puede mantener la ilusión de un negocio sustentable siempre que los nuevos inversores contribuyan con nuevos fondos, y siempre que la mayoría de los inversores no exijan el reembolso total y sigan creyendo en los activos inexistentes que supuestamente poseen. (elEconomista.es. «Esquema Ponzi: qué es - Diccionario de Economía - elEconomista.es». www.eleconomista.es. Consultado el 5 de enero de 2022).

Algunos de los primeros incidentes registrados que cumplieron con la definición moderna de esquema Ponzi fueron llevados a cabo entre 1869 y 1872 por Adele Spitzeder en Alemania, por Sarah Howe en los Estados Unidos en la década de 1880 a través del Ladies Deposit y por Baldomera Larra Wetoret en 1875 en España con la “Caja de Imposiciones”. Howe ofreció a una clientela exclusivamente femenina una tasa de interés mensual del 8 % y luego robó el dinero que las mujeres habían invertido. Finalmente fue descubierta y cumplió tres años de prisión. (Citado en Wikipedia, Esquema Ponzi, consultado 24/12/2022).

Más allá de los sistemas similares que acaecieron en el pasado, el nombre de esquema Ponzi se le atribuye al Italiano Carlo Ponzi a consecuencia de la estafa que realizó en 1920, bajo la excusa de que obtenía grandes ganancias comprando cupones de respuesta internacional de correos que se podían vender en los EEUU más caros que en el extranjero, por lo que el tipo de cambio terminaría por producir ganancias. Bajo esta excusa, logró captar miles de inversionistas que hacían largas colas para entregarle su dinero, y en realidad, Ponzi no estaba comprando los cupones, sino que estaba pagando beneficios de hasta el 100 % en tres meses utilizando el capital de los sucesivos nuevos inversionistas. (Zuckoff, Mitchell (10 January 2006). Ponzi's scheme – the true story of a financial legend. New York: Random House Trade Paperbacks. ISBN 0812968360)

El esquema de Estafa Piramidal o también conocido por su similitud como esquema Ponzi, presenta una serie de características a saber:

- Requieren una inversión inicial
- Prometen rendimientos superiores al promedio
- Para describir su estrategia de ingresos del negocio usan disfraces como “contratos de futuro”, programas de inversión de alto rendimiento o inversiones offshore, etc. o dicen que utilizan un sistema de inversión secreto para evitar dar información del esquema. Con el dinero del inversor 2 se le paga los prometidos rendimientos al inversor 1.

- Inicialmente, se pagan altos rendimientos para atraer más inversores, luego con el tiempo van disminuyendo de a poco esos rendimientos.
- Intentan minimizar los retiros, a través de nuevas ofertas de reinversión para ganar más rendimientos y así evitar que los inversores hagan sus retiros y lograr que todo lo invertido siga sin retirarse.
- Altos retornos de inversión con poco o ningún riesgo.
- Rendimientos demasiado consistentes.
- Inversiones no registradas.
- Vendedores sin licencia.
- Estrategias secretas o complejas
- Problemas con el papeleo
- Dificultad para recibir pagos
- La empresa no se encuentra registrada y controlada ante un ente regulador.
- Falta de una auditoría de confianza.

Con la finalidad de no extenderme en un análisis exhaustivo del delito de estafa, que no es el objeto del presente trabajo, pero si una parte esencial para explicar al lector la importancia de contar con mecanismos de prevención que nos permitan garantizar espacios de confianza hacia los usuarios y consumidores, en una nueva era Digital de inversiones que apenas hoy está comenzando. Y al no tener una regulación concreta sobre la materia, da lugar a un espacio enorme donde los ciberdelincuentes y oportunistas pueden actuar con un máximo de impunidad.

Tal como hace mención el tutor Leo Castela (Curso 2022), La prevención de la ciberdelincuencia en el mundo de inversiones digitales, precisa nuevas herramientas de vigilancia, control y detección de riesgos legales que permitan una mejor protección del usuario en la red, pero también en la vida real.

Continúa diciendo el tutor, cuya opinión comparto, de entre las diferentes opciones, una de la más extendidas es, sin duda la implementación de sistemas de gestión de Compliance y prevención de riesgos legales.

Y es aquí, desde este último punto, en base al cual desarrollaré brevemente el presente trabajo.

3 Responsabilidad penal de las personas jurídicas y doble vía de imputación

En julio de 2015, entró en vigor en España mediante la LO 1/2015, última reforma del Código Penal, que introduce la limitación de la responsabilidad penal de las personas jurídicas, la existencia de un programa de prevención, la existencia de un órgano de supervisión y control y la extensión del régimen de responsabilidad penal a las sociedades mercantiles estatales que ejecuten políticas públicas.

El Código Penal Español establece una doble vía para la fijación de la responsabilidad de las personas jurídicas, a saber:

- La imputación de aquellos delitos cometidos en su nombre o por su cuenta, y en su provecho, por las personas que tienen poder de representación en las mismas.
- Delitos cometidos en representación de la persona jurídica.
- Responsabilidad por aquellas infracciones propiciadas por no haber ejercido la persona jurídica el debido control sobre sus empleados. Delitos cometidos como consecuencia de la falta de control culpable de la persona jurídica sobre sus empleados. No toda persona jurídica con personalidad jurídica responde penalmente, ya que únicamente se incluyen las personas jurídico-privadas de derecho civil y mercantil.

Quedan exentas por imperativo legal (art. 31 quinquies CP):

1. Las disposiciones relativas a la responsabilidad penal de las personas jurídicas no serán aplicables al Estado, a las Administraciones públicas territoriales e institucionales, a los Organismos Reguladores, las Agencias y Entidades públicas Empresariales, a las organizaciones internacionales de derecho público, ni a aquellas otras que ejerzan potestades públicas de soberanía o administrativas.
2. En el caso de las Sociedades mercantiles públicas que ejecuten políticas públicas o presten servicios de interés económico general, solamente les podrán ser impuestas las penas previstas en las letras a) y g) del apartado 7 del artículo 33. Esta limitación no será aplicable cuando el juez o tribunal aprecie que se trata de una forma jurídica creada por sus promotores, fundadores, administradores o representantes con el propósito de eludir una eventual responsabilidad penal.

Así, están exentos de responsabilidad penal: el Estado, las Administraciones públicas territoriales e institucionales, los Organismos Reguladores, las Agencias y Entidades Públicas Empresariales, las organizaciones internacionales de derecho público y aquellas otras que ejerzan potestades públicas de soberanía o administrativas.

En el caso de las Sociedades mercantiles públicas que ejecuten políticas públicas o presten servicios de interés económico general, solamente les podrán ser impuestas las penas previstas en las letras a) y g) del apartado 7 del art. 33 CP. Pero, esta limitación no será aplicable cuando el juez o tribunal aprecie que se trata de una forma jurídica creada por sus promotores, fundadores, administradores o representantes con el propósito de eludir una eventual responsabilidad penal.

Para aquellas empresas, organizaciones, grupos o cualquier otra clase de entidades o agrupaciones de personas que, por carecer de personalidad jurídica, no estén comprendidas en el artículo 31 bis, en cuyo seno, con su colaboración o a través o por medio de ellas se cometieren delitos, no se les aplica el régimen de responsabilidad penal de las personas jurídicas, sino una o varias consecuencias accesorias a la pena que corresponda al autor del delito, con el contenido previsto en las letras c) a g) del apartado 7 del artículo 33.

Se podrá, también, acordar la prohibición definitiva de llevar a cabo cualquier actividad, aunque sea lícita, en aplicación del art. 129 CP.

Además, la persona jurídica deberá ser imputable.

La Audiencia Nacional, en su Auto de 19 de mayo de 2014, concluyó que, cuando las sociedades sean totalmente instrumentales, sin ninguna otra clase de actividad legal, o que lo sean solo meramente residual y aparente para los propios propósitos delictivos, estaremos ante personas jurídicas puramente simuladas, es decir, no reales, y que, por ello, no resultan imputables.

El TS, en la STS 154/2016, de 29 de febrero, dicta la llamada Sentencia bisiesta (en atención al día que se dictó, 29 de febrero), que es muy relevante, por recoger la primera condena penal a personas jurídicas. El pronunciamiento recoge que la persona jurídica estrictamente instrumental o pantalla, es decir, la que carece de cualquier actividad lícita y creada, exclusivamente, para la comisión de hechos delictivos, ha de ser considerada al margen del régimen de responsabilidad del artículo 31 bis, por resultar insólito pretender realizar valoraciones de responsabilidad respecto de ella, dada la imposibilidad congénita de ponderar la existencia de mecanismos internos de control y de cultura de respeto o desafección hacia la norma, respecto de quien nace exclusivamente con una finalidad delictiva que agota la propia razón de su existencia.

3.1 Catálogo de delitos

Las personas jurídicas sólo pueden incurrir en responsabilidad penal por los delitos que se incluyen en un listado cerrado, denominado también, Numerus Clausus. A fin de no entrar en un desarrollo de cada uno de ellos, si me gustaría nombrar solo a los delitos que están vinculado con la Informática, la Economía Digital y los Criptoactivos, a saber:

- Delitos contra la intimidad y allanamiento informático, Art 197 quinquies del CP Español.
- Estafas y fraudes. Art. 251 bis CP

- Insolvencias punibles Art. 261 bis CP
- Daños informáticos. art. 264 quater CP
- Delitos contra la propiedad intelectual e industrial, el mercado y los consumidores y de corrupción privada art. 288 CP
- Receptación y blanqueo de capitales. Art. 302.2 CP
- Falsedad en medios de pago. Art. 399 bis CP
- Organizaciones y grupos criminales Art. 570 del CP
- Financiación del terrorismo. art. 576.5 CP

3.2 Penas que pueden imponerse a personas jurídicas

Más allá de las penas de multas, existe un catálogo general de penas específicas susceptibles de ser impuestas a las personas jurídicas en el art 33.7 del Cp Español, con sus propias reglas de terminación en el art 66 bis del mismo cuerpo normativo.

El CP incluye, en su art. 33.7, una serie de supuestos que van desde la disolución de la persona jurídica hasta la intervención judicial, pasando por la suspensión de actividades, la clausura de locales y establecimientos, la prohibición de realización de actividades, o la inhabilitación para obtener subvenciones y ayudas públicas, contratar con el sector público y gozar de beneficios e incentivos fiscales o de la seguridad social.

3.3 Responsabilidad civil directa y solidaria de la persona jurídica

Es la consecuencia lógica del régimen general de la responsabilidad civil derivada del delito que atribuye la obligación de reparación al que participe en la comisión de la infracción y de la nueva posible consideración como tal de la persona jurídica.

3.4 Circunstancias modificativas de la responsabilidad penal

Uno de los aspectos más relevantes de la responsabilidad de las PJ, es la de los eximentes y atenuantes aplicables a las personas jurídicas, transformándose en el aspecto más interesante para las empresas.

El objetivo es implantar las medidas de prevención y control necesarias para eliminar la responsabilidad penal de la persona jurídica, en caso de comisión de delitos por parte de

sus empleados o representantes. En este punto cobran especial relevancia los programas de Compliance, es decir, los Modelos de Prevención de Delitos (MPD).

En el caso de delitos cometidos por las personas mencionadas en la letra a) del artículo 31 bis del Código Penal, su apreciación requiere el cumplimiento de una serie de requisitos:

1. Que el órgano de administración haya adoptado y ejecutado (implementado) con eficacia, antes de la comisión del delito, modelos de organización y gestión que incluyan medidas de vigilancia y control para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión.

El modelo de organización y gestión preciso para cumplir el requisito indicado exige haber sido implementado con eficacia y ser idóneo.

Además, resulta esencial que el modelo de prevención del delito (MPD) haya sido implementado antes de la comisión del delito; si el MPD es adoptado con posterioridad a la comisión del hecho delictivo, servirá como atenuante de la pena siempre y cuando haya sido implementado antes de la apertura del juicio oral (art. 31 quater d, del CP español)

2. La supervisión del funcionamiento y del cumplimiento del modelo de prevención del delito implantado debe haber sido confiada a un órgano independiente de la persona jurídica, con poderes autónomos de iniciativa y control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica.

Este órgano de la persona jurídica con poderes de control autónomos puede ser unipersonal o colegiado (Compliance Officer o Comité de Compliance). Lo relevante es que ha de tener un poder autónomo de iniciativa y control, es decir, independencia respecto de la dirección de la persona jurídica

En Resumen, Tras la reforma operada por la LO 1/2015, la responsabilidad de la persona jurídica se recoge para los delitos cometidos en el ejercicio de las actividades sociales y por cuenta y en beneficio de la persona jurídica por parte de cualquier empleado de la misma, así como de quienes con la compañía se relacionan. Al igual que sucede con los delitos cometidos por los representantes legales y administradores y directivos, los delitos cometidos por empleados deben causar beneficio directo o indirecto a la persona jurídica (cualquier ventaja), siendo irrelevante que el empleado (o el tercero relacionado con la compañía) que comete el delito quiera o no que la persona jurídica se beneficie por medio de su actuación.

Lo esencial para responder la persona jurídica es el incumplimiento grave de los deberes de supervisión, vigilancia y control. No es suficiente, para imputar responsabilidad penal a la persona jurídica, no haber ejercido el debido control, sino que es preciso que quienes ostentan facultades decisorias, de organización y control hayan incumplido gravemente sus deberes de supervisión, vigilancia y control. Constituye un plus respecto de la simple omisión del deber de vigilancia.

4 Qué es el Compliance y su necesidad

La necesidad del Compliance y el cumplimiento de las regulaciones adaptables y la lealtad del negocio, son elementos fundamentales para cualquier empresa, en especial en aquellas que operan en áreas reguladas, como la energía, la banca y la electricidad, etc., casos en que el Compliance depende de la confianza absoluta y total de sus clientes.

Podemos entender el Corporate Compliance como el conjunto de procedimientos y buenas prácticas adoptados por las empresas líderes para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención y gestión, formación, detección, minimización y control de los mismos.

“Los temas relacionados con el Compliance tienen un gran impacto reputacional para las organizaciones por cuanto está estrechamente relacionado con el cumplimiento de las normas y operar en los mercados con criterios éticos y de responsabilidad social corporativa”. (Profesor Doctor Jose Antonio Rubio Blanco, Master en Corporate Compliance, Mod 1 ed. 2021/2022, CEUPE - Madrid).

Compliance es el resultado de que una organización cumpla con todas sus obligaciones, y se hace sostenible introduciéndose en la cultura de la organización, en el comportamiento y en la actitud de las personas que trabajan en ella. Mientras mantenga su independencia, es preferible que la gestión de Compliance esté integrada con los procesos de gestión de finanzas, riesgos, calidad, medio ambiente y salud y seguridad, así como en sus requisitos y procedimientos operacionales.

Numerosas descripciones acogen el gobierno corporativo, pero, quizá, la más atractiva es la que se transcribe seguidamente y que fue realizada por Sir Adrian Cadbury :

“En su sentido más amplio, el gobierno corporativo consiste en mantener el equilibrio entre los objetivos económicos y los sociales entre los objetivos individuales y los comunitarios.

El marco de gobierno se establece con el fin de promover el uso eficiente de los recursos y, en igual medida, exigir que se rindan cuentas por la administración de esos recursos. Su propósito es lograr el mayor grado de coordinación posible entre los intereses de los individuos, las empresas y la sociedad. El incentivo que tienen las empresas y sus propietarios y administradores para adoptar las normas de gestión aceptadas a nivel internacional es que ellas los ayudarán a alcanzar sus metas y a atraer inversiones. En el caso de los Estados, el incentivo es que esas normas fortalecerán sus economías y fomentarán la probidad de las empresas.” (Cadbury Sir Adrian, prólogo de Corporate Governance and Development. Foro Mundial sobre Gobierno Corporativo. Focus 1; 2003)

4.1 La importancia y necesidad de Compliance en las organizaciones

El Corporate Compliance va a jugar un papel determinante en el seno de las empresas, con la finalidad primordial de minimizar o excluir el impacto negativo que ha de tener la nueva normativa penal sobre las organizaciones empresariales.

Los profesionales y expertos del Compliance interiorizan que el Compliance es un sistema de gestión eficaz, que abarca a toda la organización, que permite que esta demuestre su compromiso de cumplir con la normativa, incluyendo los requisitos legales, los códigos de la industria y los estándares de la organización, así como con los estándares de buen gobierno corporativo, las mejores prácticas, la ética y las expectativas de la comunidad en general.

Teniendo en cuenta que la finalidad esencial del control de cumplimiento normativo se relaciona al control del riesgo de incurrir en sanciones administrativas o judiciales, en pérdidas financieras o materiales y, sobre todo, en el daño reputacional que esto implica, lo lógico es que toda la organización se comprometa con la implantación de una efectiva función del Compliance en su estructura.

La necesidad del Compliance y, concretamente, el cumplimiento de las regulaciones adaptables y la lealtad del negocio, son elementos fundamentales para cualquier empresa, en especial en aquellas que operan en áreas reguladas, como la energía, la banca y la electricidad, telecomunicaciones, transporte o el suministro de agua. En concreto, por ejemplo, en sectores financieros, como la banca y el sector de seguros, el Compliance resulta un tema crítico porque depende de la confianza absoluta y total de sus clientes.

No obstante, el cumplimiento normativo, para cualquier organización con ánimo de lucro, implica la columna vertebral en la creación de imagen, marca y valor empresarial. De hecho, la evolución de los mercados, la regularización extrema de sectores y la globalización implica una gran complejidad en la labor de identificar y controlar las conductas.

Por estos motivos, es totalmente necesario implementar una cultura corporativa basada en los principios de honestidad, respeto y justicia.

Con más exactitud lo definió el documento que publicó en 2005 el Comité de Supervisión Bancaria de Basilea, que indica: “El riesgo de Compliance es el riesgo de que una organización pueda sufrir sanciones, multas, pérdidas financieras o pérdida de su reputación como resultado del incumplimiento de las leyes, regulaciones, normas de autorregulación o códigos de conducta que se apliquen a su actividad.”

Toda vez que el documento está dirigido a los bancos, sus definiciones y conceptos son aplicables a la perfección a cualquier organización.

4.2 Qué es un programa de cumplimiento normativo

Partimos de la necesidad de que nuestro entorno social y económico avanza de forma contundente, vertiginosa y, cada vez más, desgraciadamente, se acude a la búsqueda de soluciones rápidas a los problemas de las empresas, adquiriendo malas prácticas, que tienden a aumentar. Esta tendencia en aplicar soluciones rápidas conlleva riesgos altos y graves, vulnerando la legalidad.

En este sentido, el nivel de sanciones relacionadas con incumplimientos legales ha aumentado, y aumentará poderosamente, prueba de ellos, han sido los escándalos societarios, tales como Pescanova, la Operación Púnica, las tarjetas black de Bankia, Gowex, etc. Por ello, diferentes normas nacionales como internacionales, han hecho hincapié en la importancia de la prevención como herramienta eficaz para luchar contra estas malas prácticas, y es el motivo principal por el cual, en España (como Ejemplo), ha aterrizado el Compliance para quedarse.

Pero, ¿qué es exactamente un programa de cumplimiento normativo? Lo podríamos resumir en una frase: gobernar, diligentemente, una empresa.

Debemos tener en cuenta que cada función de la empresa constituye un pequeño universo de materias legales, conocer cada pequeño universo no brindará únicamente un valioso conocimiento de la estructura empresarial, sino también permitirá conocer con detalle los riesgos legales que les afectan, favoreciendo el prevenir, detectar y gestionarlos de forma temprana.

La cultura de control, autorregulación en materia de prevención de riesgos, a modo de ejemplo, riesgos penales, en Europa ha sido inestable. Es evidente que no en todos los países europeos se ha regulado la responsabilidad penal de las personas jurídicas, pero podemos tomar como ejemplo la legislación española y europea.

Recordemos que la persona jurídica es la organización que puede contraer derechos, obligaciones e interponer acciones legales, y que, en España, desde la reforma última de su Código Penal, puede delinquir.

Así el art 31 bis del Código Penal español (El Código Penal español actual fue aprobado por la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Este código ha sufrido multitud de modificaciones a lo largo de los años, siendo la última de las grandes reformas la producida en 2015, que entre otras implementó el Responsabilidad de las Personas Jurídicas) dicta:

1. En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables:

a) De los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma.

b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso.

2. Si el delito fuere cometido por las personas indicadas en la letra a) del apartado anterior, la persona jurídica quedará exenta de responsabilidad si se cumplen las siguientes condiciones:

1.^a el órgano de administración ha adoptado y ejecutado con eficacia, antes de la comisión del delito, modelos de organización y gestión que incluyen las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión;

2.^a la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado ha sido confiada a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica;

3.^a los autores individuales han cometido el delito eludiendo fraudulentamente los modelos de organización y de prevención y

4.^a no se ha producido una omisión o un ejercicio insuficiente de sus funciones de supervisión, vigilancia y control por parte del órgano al que se refiere la condición 2.^a

En los casos en los que las anteriores circunstancias solamente puedan ser objeto de acreditación parcial, esta circunstancia será valorada a los efectos de atenuación de la pena.

3. En las personas jurídicas de pequeñas dimensiones, las funciones de supervisión a que se refiere la condición 2.^a del apartado 2 podrán ser asumidas directamente por el órgano de administración. A estos efectos, son personas jurídicas de pequeñas dimensiones aquéllas que, según la legislación aplicable, estén autorizadas a presentar cuenta de pérdidas y ganancias abreviadas.

4. Si el delito fuera cometido por las personas indicadas en la letra b) del apartado 1, la persona jurídica quedará exenta de responsabilidad si, antes de la comisión del delito, ha adoptado y ejecutado eficazmente un modelo de organización y gestión que resulte adecuado para prevenir delitos de la naturaleza del que fue cometido o para reducir de forma significativa el riesgo de su comisión.

En este caso resultará igualmente aplicable la atenuación prevista en el párrafo segundo del apartado 2 de este artículo.

5. Los modelos de organización y gestión a que se refieren la condición 1.^a del apartado 2 y el apartado anterior deberán cumplir los siguientes requisitos:

- 1.º Identificarán las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos.
- 2.º Establecerán los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos.
- 3.º Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos.
- 4.º Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención”.
- 5.º Establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo.

6.º Realizarán una verificación periódica del modelo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios.

La importancia de este articulado, implica que una empresa implemente un programa de cumplimiento normativo (Compliance), lo que será motivo de atenuación o exención de responsabilidad penal del administrador de la sociedad mercantil en España, pero en cambio, en algunos países, como en Francia, no operan de esta forma.

Otro ejemplo es Alemania, es un país muy sensibilizado con este tema, de especial relevancia en su legislación y resulta ser un país muy puntero en la implementación de Compliance, aunque no existe en este país una responsabilidad Penal de la Persona Jurídica, sino únicamente existe un procedimiento sancionador y administrativo. (nota: En Alemania, la exigencia de culpa es requerida para que un acto sea punible penalmente. Como las personas jurídicas no pueden ser culpables, no se admite la responsabilidad penal de las personas jurídicas. Sin embargo, el sistema de responsabilidad administrativo alemán permite establecer sanciones de multas a las personas jurídicas por infracciones administrativas. Concretamente, la Ley de contravenciones o infracciones administrativas de 1968 (con las modificaciones de 1986) recoge en su § 30 la responsabilidad directa de las personas jurídicas. Esta responsabilidad presupone, en primer lugar, que alguien haya actuado como órgano con poderes de representación y, en segundo lugar, que en dicha actuación haya cometido un delito o una contravención al orden) Ref:

<http://www.knc.eus/la-responsabilidad-penal-de-las-personas-juridicas-que-operan-en-multiples-juris-dicciones/>.

Dato importante: El Consejo de Administración es el órgano que ostenta la alta dirección y, en consecuencia, el responsable de toda la supervisión de los sistemas de gestión del riesgo regulatorio y de cumplimiento normativo.

Tal como indica Neto Martin (2007) a pesar de que en el resto de Europa no todos los países tienen regulado la responsabilidad penal de la persona jurídica, bien es cierto que la cultura del cumplimiento normativo ha arraigado, y en la actualidad, aún más, en determinados sectores, como, por ejemplo, en el documento Compliance Matters. What companies can do better to respect EU Competition rules, Luxembourg 2012, así como las entidades financieras se han visto obligadas a desarrollar programas de Compliance por la normativa contra el blanqueo de capitales y, por este motivo, desde hace mucho tiempo, ya disponen de controllers, es decir, responsables de cumplimiento normativo.

A nivel de Latinoamérica y que ha servido de ejemplo para muchos países europeos, se habla que el programa de cumplimiento normativo (compliance) más desarrollado y avanzado es el de Chile.

Por ejemplo: Chile, la cual dictará la Ley 20.3931, que determina la responsabilidad penal de las personas jurídicas por delitos de lavado de activos (blanqueo de capitales), cohecho y financiamiento de terrorismo, desarrollando también Compliance en materias de libre competencia. Respecto al lavado de activos, el 10 de diciembre de 2014 se aprobó en el Congreso Nacional un proyecto de ley que contemplaba los delitos base del mismo, como el contrabando, contra la propiedad intelectual, falsedad maliciosa en los documentos presentados al Banco Central, la asociación ilícita, estafas, etc. En los delitos tributarios, por ejemplo, en casos puntuales, se permite el alzamiento del secreto bancario.

4.3 Cumplimiento normativo y cumplimiento penal

Brevemente podemos definir el cumplimiento normativo como un programa que se articula principalmente en torno a las recomendaciones y al modelo amparado por la Open Compliance and Ethics Group (OCEG), como concepto de excelencia en la gestión de procesos claves de gobierno corporativo (Governance), gestión del riesgo (risk management) y cumplimiento (Compliance), integrada en el modelo de Governance, Risk and Compliance (GRC).

4.3.1 Seis pilares fundamentales

- Liderazgo (Leadership)
- Riesgos (Risk Assessment)
- procedimientos (Standards and Controls)
- Formación (Training and Communication)

- Procedimiento sancionador (Penalization Proceedings)
- Seguimiento y Mejora (oversight)

Respecto al Cumplimiento normativo Penal, podemos decir, que el hecho de que la organización detecte un riesgo será muy positivo, tras la detección de un riesgo, siempre existe una oportunidad de conocer la empresa. En el caso de los procedimientos para detectar riesgos únicamente penales, el programa y auditoría se deberá acoger únicamente hacia esa directriz.

En estrecha relación con la responsabilidad penal de las Personas Jurídicas, el cumplimiento Normativo Penal, por ejemplo en España, es de vital importancia y obligación para todas las empresas. sobre todo, desde que ha sido legislado en el ya nombrado art 31 bis del Código Penal español (ref del 2015).

Ante cualquier incumplimiento, el penal genera un mayor impacto en nuestra sociedad, y el daño reputacional es incalculable para la organización y, por consiguiente, la subsistencia de la misma. En ese sentido, pueden imaginarse cómo en la actualidad, aun a pesar de que su asimilación es lenta, las organizaciones empiezan a mentalizarse en realizar auditorías penales.

La importancia de los programas de Criminal Compliance radica, como causa principal de criminalidad en la empresa, en la neutralización frente a conductas delictivas de los empleados que se derivan en la falta de interiorización de los valores éticos por la dirección de la organización.

La normativa vigente obliga a las empresas a implementar modelos de prevención de riesgos penales, los cuales podrán actuar como atenuantes y, en algún caso, como eximentes de la responsabilidad penal de la persona jurídica. Su importancia radica en prevenir la comisión de delitos en el seno de la empresa a través de revisión, análisis y supervisión de las actividades y procesos que se encuentran expuestos a los riesgos de comisión de delitos.

A mayor entendimiento, podemos nombrar los requisitos mínimos que deben cumplir los modelos de prevención y detección de delitos:

- Mapa de riesgos Penales: Se deberían Identificar a las actividades de la sociedad en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos. Hay que identificar y analizar los riesgos penales relevantes que afectan a la empresa, distinguiendo los riesgos propios del negocio o actividad que desarrolla la empresa de los riesgos comunes que afectarían a cualquier clase de organización. Asimismo, hay que valorar la probabilidad y el impacto en el negocio.
- Canal de Denuncias: Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención. Es decir,
 - para informar de los riesgos e incumplimientos, ha de configurarse un canal ético y un sistema de denuncias como una herramienta de comunicación en la empresa que permita la denuncia de incidencias o incumplimientos por parte de los trabajadores. El objetivo es prevenir, detectar,

investigar y resolver incumplimientos del código ético, las leyes y las normas internas de la empresa.

- **Programa de formación y sensibilización:** constituye un requisito imprescindible, a fin de que todos los miembros de la empresa conozcan el código ético y el Plan de Prevención de Delitos.
- **Recursos Financieros:** Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos. (ej: Lavado de Activos, Blanqueo de Capitales y Financiamiento del Terrorismo).
- **Protocolos de Actuación:** Establecerán los protocolos o procedimientos que concreten, en el proceso de formación, la voluntad de la empresa, la adopción de decisiones y la ejecución de las mismas en relación a aquellas.
- **Sistemas disciplinarios:** Establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo. Una política de tolerancia cero por parte de la organización demuestra el grado de implicación y el compromiso de la empresa con el Compliance. El establecimiento de una guía disciplinaria básica dirigida a los empleados puede ser útil para prevenir el delito, habida cuenta de que los empleados de la organización conocerán las consecuencias de la vulneración del Corporate Compliance.
- **Sistemas de revisión periódica:** Establecerán una verificación periódica del modelo y de su eventual modificación cuando se ponga de manifiesto infracciones relevantes de sus disposiciones o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios.
- **Plan de formación:** en cualquiera de las modalidades (coaching, presencial, online)
- **Control de las empresas del grupo, filiales y participadas:** en estos casos, los MPD han de hacerse extensivos, pudiendo tener alcance internacional.
- **Control de proveedores críticos:** el programa de Compliance ha de extenderse a proveedores críticos por la transferencia de responsabilidad.

La prevención penal exige definir políticas, procesos y controles que se proyectarán sobre las conductas de riesgos: identificar y priorizar los riesgos que pueden afectar a la entidad; identificar los procesos donde pueden residir los riesgos e identificar gaps y plan de acción para implantar controles y mitigar riesgos. También, el MPD ha de estar realmente implementado en la empresa y ser idóneo y eficaz.

4.4 Ventajas de proponer un Compliance penal

- Protege a la entidad de las consecuencias penales de un comportamiento inadecuado de sus directivos o empleados.
- Detecta riesgos y evita incidencias que podrían ocasionar sanciones administrativas o indemnizaciones civiles.
- Evita responsabilidades en el órgano de administración de la entidad por hechos cometidos por los empleados.
- Mayor valor añadido a la entidad. Se refuerzan los procesos de calidad de la entidad.
- Reputación de la imagen corporativa. Favorece la imagen de la empresa acreditando la existencia de buenas prácticas empresariales.

Por ello, y por los escándalos societarios y el innegable incremento de la sensibilidad social respecto a la ética de los negocios, un mayor número de organizaciones públicas y privadas internalizan estándares éticos y legales como protocolos de buen gobierno de obligado cumplimiento. Los riesgos a prevenir son aquellos que conllevan consecuencias como la imposición de multas y sanciones, las pérdidas de negocio, entre otras, pero, sobre todo, el daño reputacional. Evitar que la imagen corporativa resulte perjudicada es símbolo y conduce a la excelencia y ética empresarial.

4.5 Norma ISO 37301 sobre sistemas de gestión de Compliance

Este documento especifica requisitos y, además, proporciona una guía de los sistemas de gestión del compliance y prácticas recomendadas. Se pretende que tanto los requisitos como la guía que proporciona este documento sean adaptables, y su aplicación puede diferir dependiendo del tamaño y el nivel de madurez del sistema de gestión del compliance de una organización y del contexto, la naturaleza y la complejidad de las actividades y los objetivos de la organización

5 Primer intento serio de regulación europea: Reglamento MiCA

Tal como detalla el Informe del Banco De España (2022) La propuesta de reglamento MiCA considera un conjunto de reglas comunes en la UE, centradas en proveer seguridad jurídica y una adecuada protección legal de los usuarios de criptoactivos, y que serían aplicables a los emisores y a los proveedores de servicios sobre sobre estos instrumentos.

El reglamento MiCA pretende dar una regulación integral en lo relativo a los emisores de criptoactivos, plataformas de intercambio y las criptomonedas con intención de armonización de la legislación en todos los Estados Miembros de la Unión Europea.

Esta ley empezó a desarrollarse en 2020, finalmente y tras haber sido pospuesta por la complejidad técnica de la traducción a los 24 idiomas oficiales, se aprobaría en febrero de 2023, publicándose en el Diario Oficial de la Unión Europea con aplicación, en algunos casos, a los 18 meses desde su entrada en vigor a los 20 días de su publicación, es decir, entraría en vigencia aproximadamente en el año 2024.

En palabras de Bruno Le Maire - ministro de Economía, Hacienda y Soberanía Industrial y Digital de Francia -: "Los recientes avances de este sector, que está experimentando una rápida evolución, ha confirmado la urgente necesidad de una regulación a escala de la UE. El Reglamento relativo a los mercados de criptoactivos ofrecerá una mejor protección a los europeos que han invertido en esos activos y evitará que se haga un uso indebido de los criptoactivos, al tiempo que favorece la innovación para mantener el atractivo de la UE. Este Reglamento histórico pondrá fin al «Salvaje Oeste» de lo cripto y confirma el papel de la UE como organismo de normalización en lo que se refiere a temas digitales".

Para continuar diciendo que: "Actualmente, los consumidores tienen derechos muy limitados de protección o compensación, especialmente si las transacciones se realizan fuera de la UE. Con las nuevas normas, los proveedores de servicios de criptoactivos deberán respetar estrictos requisitos para proteger las billeteras de los consumidores y ser responsables en caso de que pierdan los criptoactivos de los inversores".

6 Casos de interés

Se cita el caso Hans J. Neubürger, exconsejero de la prestigiosa empresa alemana Siemens. Este ocupó el cargo de Chief Financial Officer, y durante años creó un sistema de corrupción y sobornos para conseguir pedidos e incrementar las ventas fuera de Alemania. La empresa le demandó por los daños y perjuicios ocasionados. El Tribunal Regional de Múnich valoró la eficacia del sistema Compliance de la organización. Pues bien, la sentencia alemana dictaminó que, la ignorancia de

determinados hechos no exime de responsabilidad a los cargos de una empresa ni a sus empleados, y un sistema de Compliance ineficaz supone un incumplimiento de las obligaciones del órgano de administración, incluyendo, sobre todo, la importancia en la selección, equipamiento y facultades de los responsables del Compliance en la empresa. Posterior a la sentencia, y con las fuertes presiones, Neubürger se suicidó.

En consecuencia, el Compliance y el buen gobierno van de la mano, implicando la eficacia de un buen programa y la ética de los miembros del órgano de gobierno de una organización.

http://www.abengoa.es/export/sites/abengoa_corp/resources/pdf/gobierno_corporativo/informes_anuales/2011/2011_Tomo4_IA_6.pdf

6.1 Caso Hans J. Neubürger (Siemens)

<https://www.3ccompliance.com/es/articulos/articulos/siemens-neuburger/>

6.2 Casos de interés involucrados con criptomonedas

Liberty Reserve, el golpe al blanqueo que salpica y enorgullece a Costa Rica: https://elpais.com/economia/2013/06/02/agencias/1370191735_959181.html

Costa Rica y los fondos incautados a Liberty Reserve por lavado de dinero con Bitcoin: <https://www.antilavadodedinero.com/costa-rica-y-los-fondos-incautados-a-liberty-reserve-por-lavado-de-dinero-con-bitcoin/>

Estafas piramidales: la causa One Coin ya tiene condenas a prisión: <https://www.lavoz.com.ar/sucesos/estafas-piramidales-la-causa-one-coin-ya-tiene-condenas-a-prision/>

El caso Arbistar, la mayor estafa con criptomonedas de España: <https://dirigentesdigital.com/funds-markets/criptomonedas/el-caso-arbistar-la-mayor-estafa-con-criptomonedas-de-espana>

Las víctimas de una gran 'criptoestafa' apremian al juez para empezar a juzgar: <https://www.lainformacion.com/espana/las-victimas-de-una-gran-criptoestafa-apremian-al-juez-para-empezar-a-juzgar/2874974/>

La Audiencia Nacional investigará la presunta estafa con criptos de Nimbus: 4.000 afectados y 138 millones: https://www.elconfidencial.com/mercados/2022-04-27/estafa-criptomonedas-nimbus-afectados-millones_3415127/

El juez imputa al fundador de la plataforma Kuailian por una presunta estafa piramidal con criptomonedas: <https://elpais.com/economia/2022-05-20/el-juez-imputa-al-fundador-de-la-plataforma-kuailian-por-una-presunta-estafa-piramidal-con-criptomonedas.html>

Desarticulada una red internacional acusada de estafar a 17.000 personas en España con falsas inversiones en criptomonedas: <https://elpais.com/espana/catalunya/2022-11-14/desarticulada-una-red-internacional-acusada-de-estafar-a-17000-personas-en-espana-con-falsas-inversiones-en-criptomonedas.html>

Denuncian a empresa Mind Capital en España por estafa de criptomonedas: <https://es.beincrypto.com/denuncian-empresa-mind-capital-espana-estafa-criptomonedas/>

Cómo es la estafa piramidal crypto que logró hacerse de más de 300 millones de dólares: <https://www.forbesargentina.com/money/como-estafa-piramidal-crypto-logro-hacerse-mas-300-millones-dolares-n19806>

Las estafas con criptomonedas se multiplican y dejan atrapados a miles de inversores: https://www.eldiarioar.com/economia/estafas-criptomonedas-multiplican-dejan-atrapados-miles-inversores_1_9770036.html

6.3 El boom de las macroestafas de criptos ante la Audiencia Nacional

Bankman-Fried, el cerebro de FTX acusado de fraude, en libertad bajo fianza de 250 millones de dólares: <https://elpais.com/economia/2022-12-22/los-principales-socios-del-fundador-de-ftx-s-e-declaran-culpables-de-fraude-por-la-quebra-de-la-compania.html>

7 Conclusiones

Con la nueva Revolución tecnológica que causo la implementación de las criptomonedas y la aparición de la Blockchain, resurgieron de entre las cenizas los viejos modelos de estafas piramidales, aumento la facilidad de los metodos financieros de Blanqueo de Capitales y Financiamiento del Terrorismo, como otros delitos típicos que tambien se encuentran en el sistema tradicional. Al ser un mundo descentralizado (DeFi), los ciberdelincuentes encontraron un espacio donde pueden delinquir con casi total impunidad, por las ventajas que posee para ellos un mundo descentralizado sin ningún control por parte del Estado y de parte de las instituciones

privadas que puedan ejercer el poder de policía. Quedando a merced de ellos, todos los usuarios, consumidores e inversionistas que quieran operar en el mundo cripto.

Como podemos apreciar, a través de los casos que se han puesto como ejemplos, miles de usuarios han sido estafados por cifras millonarias. Y los cuales, han utilizado como medio de inversión las criptomonedas, puestas a disposición de determinadas plataformas que han prometido rendimiento muy altos sobre la media de las inversiones tradicionales, siendo no menos que estafas piramidales o Ponzis.

Tal vez, por desconocimiento, también por ambición, pero de una u otra manera han sido despojados en muchos casos, de la totalidad de sus ahorros por escrupulosos mal intencionados que han visto la oportunidad de hacerse de lo ajeno a través del engaño y falsas promesas, aprovechando el desconocimiento ajeno y la impunidad que hoy reina en un sistema descentralizado.

Debemos reconocer que las cadenas de bloques públicas son transparentes. Al no estar controladas por una sola entidad, pueden aportar una infraestructura neutral, independiente e inalterable para las transacciones financieras. El código se almacena y se ejecuta en un sistema abierto. Todos los datos son accesibles y verificables. Tanto investigadores como autoridades pueden analizar las transacciones, hacer estudios empíricos y medir el riesgo en tiempo real. El desarrollo y aplicación de los smartcontract, ha facilitado operaciones más ágiles y mucho menos costosas, pero quedan a merced de errores o baches informáticos que den lugar al acceso y modificación de ellos sin las debidas autorizaciones.

El Mundo DeFi, desde mi humilde opinión, es el futuro de las finanzas y el acceso de todas las personas que hoy dudan en acceder por diversas cuestiones, la base de todo este desarrollo que recién comienza es la blockchain y los Criptoactivos.

Pero he aquí el quid de la cuestión, ¿podrá existir un 100 % un sistema descentralizado? Pues de mi parte no creo que sea posible en los próximos años, es necesario que la descentralización sea acompañada con un marco centralizado de regulación y es aquí donde comparto la opinión del tutor Leo Castela (Curso Criptoactivos 2022, Mod Criptoactivos y Prevención del Delito) en que el Compliance es la vía ética, madura y correcta para que las partícipes de la descentralización puedan ingresar y operar con más seguridad.

El Compliance y la prevención de riesgos legales, podrán disminuir el riesgo social, jurídico y económico tanto para el usuario en la red como también en la vida real. Aplicándose herramientas de vigilancia, control y detección de riesgos legales. Así se podrá dar mayor seguridad a los usuarios, logrando espacios de confianza y seguridad en la Red.

Es decir, la implementación de sistemas de gestión de Compliance y prevención de riesgos legales, sería el camino correcto para lograr una centralización que brinde seguridad al usuario, y una mayor operatividad y participación en un ambiente de confianza dentro de la descentralización de la red y las fianzas (DeFi).

8 Recursos bibliográficos

8.1 Bibliografía básica

- Guía Santander 2022. <https://www.santander.com/es/stories/guia-para-saber-que-son-las-c-riptomonedas>
- KNC. La responsabilidad penal de las personas jurídicas que operan en múltiples jurisdicciones. <http://www.knc.eus/la-responsabilidad-penal-de-las-personas-juridicas-que-operan-en-multiples-jurisdicciones/>
- NETO MARTIN, A. ¿Americanización o armonización del derecho penal económico europeo?, Revista Penal, 2007.
- NETO MARTIN, A. La responsabilidad penal de las personas jurídicas: un modelo legislativo. Madrid, 2008.
- CASANOVAS, A. Control legal interno. Madrid: Grupo Wolters Kluwer Editorial La Ley, S.A., 2012.
- DÍAZ GÓMEZ, A. El modelo de responsabilidad criminal tras la LO 5/2010. Revista Electrónica de Ciencia Penal y Criminología, agosto 2011.
- Leo Castela, Juan Ignacio. Módulo: Criptoactivos y Prevención del Delito, Curso Superior de Inversiones Digitales y Criptoactivos, Fundación Salamanca, 2022.

8.2 Bibliografía complementaria

- Conceptos Jurídicos. Código Penal, artículo 31 bis. <https://www.conceptosjuridicos.com/codigo-penal-articulo-31-bis/>
- ARMENDÁRIZ LEÓN, C. La responsabilidad penal de las personas jurídicas. A propósito de las primeras resoluciones del Tribunal Supremo, 2016.
- CARRASCO PERERA, A. y ALMARCHA JAIME, J. Alcance de la responsabilidad penal de la persona jurídica según el Tribunal Supremo, 2016.
- CONTRERAS, J. L. Compliance Program: Códigos Éticos empresariales, 2016.
- LEFEBVRE, F. Memento Práctico Procesal Penal, 2015.
- LEO-CASTELA, J. I. Gestión de riesgos legales y Compliance Corporativo. Tirant lo Blanch, 2021.

- PUYOL MONTERO, J. Corporate compliance y la responsabilidad penal de las personas jurídicas.
- NACIONES UNIDAS. Informe de Naciones Unidas sobre el coste que representa la desregulación de criptoactivos en la economía global, 2020.

8.3 Otros recursos

- Internet, normas ISO y Código Penal español.

Acerca de Marcos Romero Perin

Marcos Romero Perin es abogado, con trayectoria profesional vinculada al Derecho Penal, Corporate Compliance, prevención de riesgos legales, economía digital, criptoactivos y LegalTech. Integra experiencia jurídica, formación académica y tecnología aplicada para analizar riesgos, orientar decisiones y promover una comprensión más clara y preventiva del Derecho en entornos digitales.

www.marcosromeroperin.com
linkedin.com/in/marcosromeroperin
instagram.com/marcosromeroperin
x.com/MRomeroPerin

Este documento forma parte del archivo académico y profesional de Marcos Romero Perin sobre economía digital, criptoactivos, Compliance, prevención de riesgos legales y tecnología aplicada al Derecho.