Evolución del término *compliance* en el Perú

Doris Rocío Alvaro Cutipa-Flores*
Pontificia Universidad Católica del Perú

Recibido: 24 de marzo del 2025 / Aceptado: 13 de abril del 2025
doi: https://doi.org/10.26439/iusetpraxis2025.n060.7843

RESUMEN. Los actuales sistemas de cumplimiento (*compliance*) al interior de las organizaciones buscan protegerlas de diversos riesgos. El principal de estos es el reputacional, aunque se cuentan también como riesgos el operacional, el financiero, el empresarial y el laboral. En el presente artículo abordaremos los principales sistemas actuales de cumplimiento, los cuales abarcan diversos campos como el sistema de prevención del lavado de activos, el modelo de prevención de delitos, los sistemas de ética e integridad, y el sistema de protección de datos personales. Todos estos tienen como elemento común la gestión de riesgos, el cumplimiento de la normativa, el seguimiento de prácticas de buen gobierno corporativo y la difusión de buenas prácticas empresariales hacia la sociedad. Resulta imperativo que las siguientes generaciones comprendan la relevancia del cumplimiento de las reglas y el cuidado de su reputación, y que tengan la conciencia de hacer siempre las cosas bien.

PALABRAS CLAVE: cumplimiento / prevención / normas / riesgos / ética / integridad

* Magíster en Derecho de los Negocios por la Universidad Francisco de Vitoria de Madrid. Abogada por la Pontificia Universidad Católica del Perú. Especialista en derecho bancario, financiero, societario, contractual y regulatorio. Es socia del estudio Barrios & Fuentes Abogados y experta en prevención del lavado de activos y *compliance*. Ha sido gerente legal del Fondo Mivivienda y de cumplimiento en diversas entidades bancarias como ICBC Perú Bank y HSBC Bank Perú. Asimismo, ha sido abogada *senior* en Interbank y *compliance officer* en Standard Chartered Bank. Inició su carrera en derecho en Citibank del Perú. Ha sido catedrática universitaria desde el 2006 en Derecho Empresarial en la Universidad Peruana de Ciencias Aplicadas y docente de Derecho Corporativo en la Universidad San Ignacio de Loyola hasta el 2020. Contacto: dalvaro@bafur.com.pe

COMPLIANCE TERM EVOLUTION IN PERÚ

ABSTRACT. Current compliance systems within the organizations seek to protect them from various risks, the most important of which is the reputational risk; however, the risks involved are the operational risk, financial risk, corporate risk, labor risk, which also affect the organizations, considering their own sector in the market, for example, the environmental risk, technological risk, biological risk as well as the chemical risk related to the effects of financing of weapons of mass destruction . In this article we will discuss the main compliance systems, which cover diverse fields such as the anti-money laundering system, the crime prevention model, ethics and integrity systems, and the personal data protection system, all of which have the risk management, the fulfilment of the regulation, monitoring of corporate governance practices and the dissemination of good business practices in favor of the society as the common factor. It is imperative that next generations understand the importance of following rules and protecting their reputation, having awareness of always doing the right thing.

KEYWORDS: compliance / prevention / regulations / risks / ethics / integrity

1. INTRODUCCIÓN

En el ecosistema actual se habla diariamente sobre *compliance*. La palabra *compliance* es un anglicismo que se define como el cumplimiento de algo. Siendo coherentes con la traducción del término, todos podríamos dedicarnos al *compliance*, debido a que comprende el cumplimiento de una cosa que resulta obligatoria; y, en el caso del mundo jurídico, el cumplimiento de cualquier norma que sea de carácter imperativo o que constituya una política empresarial interna que sea una regla para todos sus miembros.

No obstante, la práctica del derecho nos demuestra que el término *compliance* ha venido ampliándose cada vez más. En el año 2000, por ejemplo, entendíamos por *compliance* a la normativa relacionada al sistema de prevención del entonces denominado lavado de activos. En ese momento, dicho sistema —aún incipiente— era obligatorio únicamente para las entidades del sistema financiero local supervisadas por la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS). Es en el 2000 cuando el Perú adopta los estándares del Financial Action Task Force (Grupo de Acción Financiera Internacional, GAFI), es decir, las recomendaciones respecto a diversas materias del sistema de prevención del lavado de activos y financiamiento del terrorismo, en la búsqueda, principalmente, de la tipificación del delito de lavado de activos. Si en ese momento nos referíamos al *compliance*, era altamente probable que las personas entendieran que hablábamos de un sistema de prevención que implicaba el conocimiento del cliente, la contraparte, las transacciones involucradas y el establecimiento de determinadas políticas al interior de las organizaciones reguladas por la SBS, según lo recomendado por GAFI.

Las empresas subsidiarias del exterior, o las sucursales de las empresas extranjeras, sea que estuviesen en el sistema financiero o no, sí tenían una definición ampliada del término *compliance*; es decir, además de lo anterior, incluían el cumplimiento de reglas de conducta que iban desde el ingreso del personal y los programas de entrenamiento hasta el código de vestimenta, lo que incluía reglas para la prevención de conductas indeseadas —delictivas o no—, así como el cuidado de las normas de ética e integridad corporativa.

Como vemos, no ni existe, en forma concreta, una delimitación del término *compliance*. Pero, tanto antes como en el 2025, el término refiere a la revisión, supervisión y seguimiento del cumplimiento de normas internas y externas que afectan a una organización o empresa, local o extranjera, la cual debe cuidar el riesgo reputacional que su incumplimiento normativo pueda acarrear. Esta definición puede no ser compartida por todos, pero es propuesta aquí sobre la base de la experiencia profesional —de quien escribe— en cargos gerenciales en empresas multinacionales e internacionales, en una empresa de capital estatal y en un estudio de abogados, y de la labor de asesoría permanente a diversas entidades y corporaciones, peruanas y extranjeras, en materia de *compliance*, ética e integridad. Si lo que se busca, entonces, es no llegar al daño reputacional y responder ante

los accionistas sobre las acciones de mitigación al respecto, el sistema de *compliance* debe ser transversal a toda la organización e involucrar a cada miembro de la misma.

Si circunscribimos el término a lo que hoy vivimos, podría mencionar que los siguientes campos son los que se consideran *compliance*: el sistema anticorrupción o de prevención de delitos; el sistema de prevención del lavado de activos, financiamiento del terrorismo y financiamiento a la proliferación de armas de destrucción masiva; el sistema de cumplimiento normativo de las reglas generales que se aplican a la empresa y que están determinadas por la regulación, la ética y la integridad; el sistema de protección de datos personales; el sistema de prevención de conductas anticompetitivas y protección al consumidor; el sistema de prevención de riesgos laborales; y el sistema de cumplimiento tributario. Seguramente, desde otras perspectivas y con el transcurso de los años, podremos hablar de más campos del *compliance*. En el presente artículo solo se abordará el *compliance* aplicado a los cuatro primeros campos: para la prevención del delito, para la prevención del lavado de activos, para el cumplimiento de la normativa regulatoria y para la protección de datos personales.

Al interior de las empresas, la supervisión y monitoreo de todas estas tareas deberían estar a cargo de un funcionario de *compliance*, un comité de *compliance* o de ética y, en caso de existir, un regulador gubernamental. En el Perú, la supervisión centralizada de los sistemas de *compliance* no existe, a excepción de las empresas reguladas por la SBS; y aquellas que pertenecen a sectores que la normativa peruana ha elegido por su riesgo de lavado de activos, financiamiento del terrorismo y a la proliferación de armas de destrucción masiva, las cuales están supervisadas por la Unidad de Inteligencia Financiera del Perú (UIF), una superintendencia adjunta de la SBS, pero que es nombrada por la normativa aplicable como la supervisora en materia de prevención de dichos sectores. Finalmente, también se contempla como excepción la regulación de la Autoridad Nacional de Protección de Datos Personales, la que cada vez asume mayor protagonismo dado que sus competencias alcanzan a todos los sectores del mercado que dan tratamiento a datos de personas naturales, cuya protección se origina en la Constitución Política del Perú de 1993.

En cuanto a la normativa sobre prevención de delitos, tenemos a la Superintendencia del Mercado de Valores (SMV). Sin embargo, la SMV no es una reguladora del sistema de *compliance*, sino que es la autoridad que emitirá un informe técnico en caso de que exista una investigación a cargo de un fiscal del Ministerio Público. El fiscal en mención será quien le solicite la emisión de dicho informe a la SMV respecto a la adopción, existencia y funcionamiento de un modelo de prevención de delitos al interior de la organización que sea objeto de la mencionada investigación.

Como vemos hasta aquí, un sistema de *compliance* puede o no estar regulado o supervisado, pero lo que sí es claro es que debe existir para cuidar la reputación de

la empresa y sus miembros. Lo peor que le puede pasar a una organización a nivel patrimonial es poner en riesgo su reputación. Las sanciones existen y existirán, así como las multas serán pagadas, aunque coercitivamente; sin embargo, el daño a la reputación, a la imagen y a la confianza es invaluable y podría tomar muchos años en ser reivindicado.

Cabe precisar que, para que tales sistemas de *compliance* existan, las regulaciones y las buenas prácticas indican que se debe designar a un oficial de cumplimiento (*compliance officer*) o a un encargado de prevención de delitos, según el sistema de cumplimiento que la organización adopte. A estos *officers* los denominaremos en forma genérica funcionarios de *compliance*. El funcionario de *compliance* que se designe requiere experiencia, conocimiento, determinadas competencias de negociación, un *seniority* que le permita llegar a todos los niveles del organigrama empresarial y, asimismo, la protección y respaldo de la alta gerencia y el directorio. Necesitará constante capacitación en el giro de negocios de las empresas y su participación en el lanzamiento de los nuevos productos o servicios será determinante para advertir los riesgos desde un punto de vista experto.

El *senior management* (alta gerencia) y el *board of directors* (directorio) constituyen órganos claves de la empresa para que un sistema de *compliance* funcione y se mantenga en el tiempo, activo, actualizado y acorde al tamaño y necesidades de la organización y del mercado en el que se desarrolla. Pasemos, entonces, a ver el campo de cada uno de los sistemas de *compliance* que se han mencionado en párrafos anteriores.

2. SISTEMA DE PREVENCIÓN DE DELITOS O MODELO DE PREVENCIÓN DE DELITOS

El origen normativo del modelo de prevención de delitos está en la Ley 30424, del 21 de abril del 2016, ley que regula la responsabilidad administrativa de las personas jurídicas en el proceso penal, y en su reglamento, aprobado el 9 de enero del 2019 mediante el Decreto Supremo 002-2019-JUS (su última modificación es del 25 de febrero del 2025 a través del Decreto Supremo 002-2025-JUS). Esta normativa busca prevenir, detectar y mitigar la comisión de delitos, así como la promoción de la integridad y transparencia en la gestión de las personas jurídicas.

La Ley 30424 permite a las empresas y personas jurídicas en general acceder al beneficio de eximir, o atenuar, la responsabilidad administrativa que les correspondería en los supuestos de una investigación o proceso penal por la comisión de alguno de los delitos establecidos por la norma en mención, si adoptan un modelo de prevención de delitos. Son diversos los delitos que incluye la Ley 30424: regula al cohecho, el tráfico de influencias, la contabilidad paralela, la extracción ilegal de bienes culturales, entre otros. Al momento de su promulgación esta norma fue conocida como la regulación anticorrupción; sin embargo, con la lista de diferentes delitos hoy incluidos, ya no puede ser denominada así.

El modelo de prevención de delitos (MPD) es el conjunto de normas, reglas, actividades, procesos y acciones que adopta voluntariamente una persona jurídica o una empresa, a fin de establecer un sistema de control interno preventivo ante la potencial comisión de delitos. A través de la debida diligencia, este conjunto de normas protege internamente a la persona jurídica, además de que le otorga el conocimiento y el entrenamiento necesarios para que se conozca qué actos y actividades califican como delitos en el marco de la ley y cuáles son las medidas que mitigan el riesgo de comisión de ellos, así como los medios para denunciarlos.

El MPD no eliminará la responsabilidad personal de quien cometa un delito y solo protege a la persona jurídica, en la medida de que el propio modelo exista, se encuentre en funcionamiento y sea debidamente actualizado. Ante un proceso de investigación en el que se vea involucrada una persona jurídica, la SMV emitirá un informe técnico sobre la implementación y funcionamiento del modelo de prevención de delitos. El informe que emita la SMV será valorado por el fiscal a cargo y por el juez competente sin ser vinculante. Serán estos últimos quienes tomen la decisión sobre el carácter eximente o no respecto de la responsabilidad de la persona jurídica.

Un cambio reciente y muy relevante en la normativa acerca del modelo de prevención de delitos es el que introduce la Ley 31740, vigente desde el 13 de mayo del 2023, al establecer que el referido modelo es inaplicable para el *senior management*, es decir, a los socios, directores y funcionarios que cometan los delitos y tengan poder de control, dirección y decisión en la organización. Ante esta situación, corresponderá que el juez imponga una multa. Es la propia ley la que establece la forma de imposición y cálculo de las multas.

Al respecto, Reaño Peschiera & Medina Frisancho (2023) precisan que

> la más reciente modificación a la Ley 30424 impide apreciar los efectos eximentes del modelo de prevención de delitos cuando en la práctica indebida hayan intervenido socios, accionistas, directores, administradores de hecho o derecho, representantes legales o apoderados de la persona jurídica, con 'capacidad de control', entendida como poder de decisión sobre el concreto ámbito de gestión en el que tuviera lugar la infracción penal. Así, la Ley 31740, publicada el 13 de mayo del 2023, ha introducido una modificación que desfigura el régimen de atribución de responsabilidad corporativa por la comisión de delitos, al punto de volverlo irreconocible para el legislador que en 2016 instauró en el Perú el novedoso modelo de responsabilidad autónoma de personas jurídicas al promulgarse la Ley 30424. (p. 332)

Desde esta perspectiva, esperamos que el legislador evalúe retornar al ámbito de responsabilidad inicial sin aislar al *senior management*, situación que hoy podría desincentivar el establecimiento de un sistema de *compliance* organizacional.

3. SISTEMA DE PREVENCIÓN DEL LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO

El sistema de prevención del lavado de activos y financiamiento del terrorismo es aplicable a los denominados sujetos obligados a informar a la UIF. El origen normativo de este sistema se encuentra en la Ley 27693, ley del 12 de abril del 2002 que crea la UIF, y en su reglamento, creado mediante el Decreto Supremo 020-2017-JUS el 6 de octubre del 2017. La UIF es una superintendencia adjunta que forma parte de la SBS, por lo que toda la regulación de desarrollo se emite a través de resoluciones de esta última. El sistema financiero tiene su propia normativa, así como los demás sectores —denominados como sujetos obligados fuera del sistema financiero— cuentan con sus propias resoluciones emitidas por la SBS.

En el caso de los sectores bajo la supervisión de la SMV, es esta quien emite la normativa en el sistema de prevención del lavado de activos y financiamiento del terrorismo. El 2025, la SMV ha modificado su regulación aplicable a los sujetos obligados dentro del mercado de valores. Todos los sujetos obligados deben adoptar un sistema de prevención del lavado de activos y financiamiento del terrorismo basado en la administración de riesgos, a través de la designación de un oficial de cumplimiento, la creación de políticas internas y de conducta, la identificación de operaciones inusuales, el reporte a la UIF de operaciones calificadas como sospechosas y la emisión de un informe anual, entre otras obligaciones propias de cada sector.

¿Quiénes son los sujetos obligados para la ley peruana? Existe un régimen general y un régimen simplificado. La lista del régimen general es larga. De conformidad con el artículo 8 de la Ley 27693, su reglamento y la normativa de desarrollo de la SBS y de la SMV, la lista se refiere a

> 1. Las empresas del sistema financiero y del sistema de seguros y las demás comprendidas en los artículos 16 y 17 de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, Ley 26702.
>
> 2. Las empresas emisoras de tarjetas de crédito.
>
> 3. Las cooperativas de ahorro y crédito.
>
> 4. Las que se dedican a la compraventa de divisas.
>
> 5. Las que se dedican al servicio postal de remesa y/o giro postal.
>
> 6. Las empresas de préstamos y/o empeño.
>
> 7. Los administradores de bienes, empresas y consorcios.

8. Las sociedades agentes de bolsa, las sociedades agentes de productos y las sociedades intermediarias de valores.

9. Las sociedades administradoras de fondos mutuos, fondos de inversión y fondos colectivos.

10. La Bolsa de Valores, otros mecanismos centralizados de negociación e instituciones de compensación y liquidación de valores.

11. La bolsa de productos.

12. Las que se dedican a la compra y venta de vehículos, embarcaciones y aeronaves.

13. Las que se dedican a la actividad de la construcción y/o la actividad inmobiliaria.

14. Los agentes inmobiliarios.

15. Las que se dedican a la explotación de juegos de casinos y/o máquinas tragamonedas, y/o juegos a distancia utilizando el internet o cualquier otro medio de comunicación, de acuerdo con la normativa sobre la materia.

16. Las que se dedican a la explotación de apuestas deportivas a distancia utilizando el internet o cualquier otro medio de comunicación, de acuerdo con la normativa sobre la materia.

17. Las que se dedican a la explotación de juegos de lotería y similares.

18. Los hipódromos y sus agencias.

19. Los agentes de aduana.

20. Los notarios públicos.

21. Las empresas mineras.

22. Las que se dedican al comercio de joyas, metales y piedras preciosas, monedas, objetos de arte y sellos postales.

23. Los laboratorios y empresas que producen y/o comercializan insumos químicos y bienes fiscalizados.

24. Las empresas que distribuyen, transportan y/o comercializan insumos químicos que pueden ser utilizados en la minería ilegal, bajo control y fiscalización de la Superintendencia Nacional de Aduanas y Administración Tributaria.

25. Las que se dedican a la comercialización de las maquinarias y equipos que se encuentran comprendidos en las subpartidas nacionales 84.29, 85.02 y 87.01 de la clasificación arancelaria nacional.

> 26. Las que se dedican a la compraventa o importaciones de armas y municiones.
>
> 27. Las que se dedican a la fabricación y/o la comercialización de materiales explosivos.
>
> 28. Las sociedades administradoras, conforme al financiamiento participativo financiero.
>
> 29. Los abogados y contadores públicos colegiados que, de manera independiente, y las personas jurídicas, cuyo objeto social es la prestación de servicios jurídicos, legales y/o contables, que realizan o se disponen a realizar en nombre de su cliente o por cuenta del mismo, de manera habitual, las siguientes actividades: (a) compra y venta de bienes inmuebles; (b) administración del dinero, valores, cuentas del sistema financiero u otros activos; (c) organización de aportaciones para la creación, operación o administración de personas jurídicas; (d) creación, administración y/o reorganización de personas jurídicas u otras estructuras jurídicas; (e) compra y venta de acciones o participaciones sociales de personas jurídicas. La información que estos sujetos obligados proporcionan a la UIF-Perú se restringe a aquella que no se encuentra sujeta al secreto profesional.
>
> 30. Los proveedores de servicios de activos virtuales.

De todos los sistemas de *compliance* mencionados, este es el más altamente regulado.

4. SISTEMA DE CUMPLIMIENTO EN ÉTICA E INTEGRIDAD

En cuanto a normas de ética e integridad, así como respecto de políticas internas de organizaciones que no tienen una normativa externa obligatoria, el sistema de *compliance* juega un rol de autorregulación. Pensemos, por ejemplo, en una política sobre conflicto de intereses para evitar riesgos en las contrataciones y decisiones; o en una política de regalos y atenciones, la cual impediría que un obsequio quiebre la voluntad de un funcionario de la empresa; o en un código de vestimenta o una política antidrogas o alcohol; no son normas del sistema jurídico peruano que impacten o generen una sanción, pero las empresas prefieren adoptar medidas disciplinarias y de conocimiento generalizado para tener ambientes de trabajo más sanos y transparentes, lo que redundará positivamente en la reputación corporativa. Recordemos que un mundo globalizado reconoce en forma positiva la adopción voluntaria por parte de las organizaciones de sistemas internos de *compliance* para evidenciar el apetito de riesgo, el respeto a las regulaciones, la inexistencia de tolerancia a determinados incumplimientos, y todo con el mismo fin de comunicar la importancia de la buena reputación y cuidar la creación de relaciones comerciales con contrapartes informadas y que se sometan a determinadas reglas.

5. SISTEMA DE PROTECCIÓN DE DATOS PERSONALES

Su origen normativo está en la Ley 29733, Ley de Protección de Datos Personales, aprobada el 3 de julio del 2011, y en su reglamento, aprobado mediante el Decreto Supremo 016-2024-JUS, vigente desde el 30 de marzo del 2025. Si bien es cierto que ya desde 1993, con el artículo 2, numeral 6, de la Constitución Política del Perú, se reconocía el derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministrasen informaciones que afecten la intimidad personal y familiar, no es sino con la Ley 29733 que se desarrolla tal precepto constitucional con amplitud.

La finalidad de esta normativa de *compliance* es preservar, custodiar y mantener en reserva la información que es de propiedad de las personas naturales, con el fin de evitar abusos, prevenir delitos y promover la confianza en el entorno digital. Es una normativa muy ligada a la ciberseguridad, porque, si bien los datos de las personas también se almacenan y custodian en soporte físico, su gestión principal se realiza en soporte electrónico, administrados en plataformas digitales a las que podría acceder cualquier tercero con conocimiento tecnológico o con manejo de herramientas de inteligencia artificial.

De acuerdo con esta normativa de protección de datos personales, cierta información califica como sensible, relativa a la salud, a la esfera íntima o afectiva, involucra datos biométricos, ingresos económicos, hábitos personales, etcétera, cuya liberación indebida podría poner en grave riesgo a una persona que los ha brindado con la convicción de que estos no serán compartidos o divulgados.

En materia de protección de datos personales, surge el término *consentimiento*, que no es más que una autorización expresa para el tratamiento de datos bajo determinadas reglas que disponga la política de privacidad de quien recabe o solicite la entrega de información personal. Un antecedente relevante es el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, aprobado el 27 de abril del 2016, sobre protección de datos personales. En su artículo 6 se resalta la licitud del tratamiento de datos y se hace énfasis en que, salvo por las excepciones expresas de un requerimiento de las autoridades o el cumplimiento de una obligación legal, el consentimiento es la condición más relevante para dar uso, proceso, transferencia, entre otros, a los datos de los individuos. Claramente, la Unión Europea, con su normativa de desarrollo en los países miembros, difunde esta necesaria protección del derecho a la privacidad, la cual es un referente para diversos ordenamientos jurídicos, incluido el peruano.

Es así que, en el Perú, las empresas se someten a múltiples obligaciones que incluyen el registro de los bancos de datos, la designación de un oficial de protección de datos personales, la comunicación de los incidentes de seguridad, el permiso para ejercer determinados derechos denominados ARCO (acceso, rectificación, cancelación,

oposición), poner a disposición de la autoridad la información que esta requiera ante una fiscalización *in situ* o *extra situ*, a la comunicación del traslado de la información personal fuera del lugar de obtención, incluyendo el extranjero, entre otras.

Desde el 2025, se han agregado dos nuevos principios para las organizaciones que traten datos personales, que son el de responsabilidad proactiva y el de transparencia. El primero se refiere a que el tratamiento de datos se dará aplicando diferentes medidas que sean demostrables para el cumplimiento de la normativa, mientras que el segundo se refiere a que el titular de los datos debe contar con información permanente, comprensible y clara para que conozca y comprenda sus derechos. El lugar adecuado para explicarle a los usuarios y consumidores el uso de sus datos es la política de privacidad, la cual no exonera de la obtención del consentimiento del titular para tratar sus datos, al ser momentos y oportunidades diferentes. Si bien las sanciones impactarán en la reputación organizacional, será la pérdida de la confianza lo que ocasionará mayor daño.

¿Qué más podemos considerar como *compliance*? Tal como lo indiqué al inicio, en puridad, podríamos considerar todo lo que implica el cumplimiento de una norma o regla que afecta a una organización y cuyo incumplimiento impactará en la reputación empresarial. Quizá en unos años veremos que el *compliance* abarque más ramas y regresaremos a este trabajo académico para actualizarlo como corresponda.

6. CONCLUSIONES

1. El *compliance* puede abarcar diferentes áreas que impactan en las empresas, principalmente, en el riesgo reputacional.
2. Tradicionalmente, los sistemas de *compliance* se han referido al sistema de prevención del lavado de activos, sistemas anticorrupción o prevención de delitos, sistemas de ética e integridad y sistemas de protección de datos personales.
3. Cada sistema de *compliance* tiene su propia regulación. En el caso de la SBS y la UIF la regulación y supervisión es constante. En cuanto al sistema de prevención de delitos y al sistema de ética e integridad, no existe un ente regulador gubernamental. La Autoridad de Protección de Datos Personales sí regula, fiscaliza y sanciona a todos los sectores en materia de protección de datos personales.
4. El funcionario de *compliance* debe contar con características y cualidades que permitan hacer sostenible su posición e impacten positivamente en la organización.
5. La alta gerencia debe tener un compromiso genuino con los sistemas de *compliance* adoptados y con la integridad corporativa.

REFERENCIAS

Constitución Política del Perú. Art. 2. 29 de diciembre de 1993 (Perú).

Decreto Supremo 002-2019-JUS. Por el cual se aprueba el reglamento de la Ley 30424, ley que regula la responsabilidad administrativa de las personas jurídicas [Ministerio de Justicia y Derechos Humanos]. 9 de enero del 2019. Diario Oficial el Peruano. https://cdn.www.gob.pe/uploads/document/file/523569/reglamento-de-la-ley-n-30424.pdf.pdf?v=1581955249

Decreto Supremo 002-2025-JUS. Por el cual se modifica e incorpora artículos al reglamento de la Ley 30424 [Ministerio de Justicia y Derechos Humanos]. 25 de febrero del 2025. Diario Oficial el Peruano. https://img.lpderecho.pe/wp-content/uploads/2025/02/Decreto-Supremo-002-2025-JUS-LPDerecho.pdf

Decreto Supremo 016-2024-JUS. Por el cual se aprueba el nuevo reglamento de la Ley 29733, Ley de Protección de Datos Personales, el cual entrará en vigencia a partir del 30 de marzo del 2025 [Ministerio de Justicia y Derechos Humanos]. 30 de noviembre del 2024. https://img.lpderecho.pe/wp-content/uploads/2024/11/Decreto-Supremo-016-2024-JUS-LPDerecho.pdf

Decreto Supremo 020-2017-JUS. Por el cual se aprueba el reglamento de la Ley 27693, ley que crea la Unidad de Inteligencia Financiera (UIF – Perú) [Ministerio de Justicia y Derechos Humanos]. 6 de octubre del 2017. https://www.sbs.gob.pe/Portals/5/Decreto%20Supremo%20N%20020-2017-JUS.pdf

Ley 27693 del 2002. Ley que crea la Unidad de Inteligencia Financiera. 12 de abril del 2002. Diario Oficial El Peruano. https://www.leyes.congreso.gob.pe/documentos/Leyes/27693.pdf

Ley 29733 del 2011. Ley de Protección de Datos Personales del Perú. 3 de julio del 2011. Diario Oficial El Peruano. https://www.leyes.congreso.gob.pe/documentos/leyes/29733.pdf

Ley 30424 del 2016. Ley que regula la responsabilidad administrativa de las personas jurídicas por el delito de cohecho activo transnacional. 21 de abril del 2016. Diario Oficial El Peruano. https://img.lpderecho.pe/wp-content/uploads/2023/07/Ley-30424-LPDerecho.pdf

Ley 31740 del 2023. Ley que modifica la Ley 30424. 13 de mayo del 2023. Diario Oficial El Peruano. https://img.lpderecho.pe/wp-content/uploads/2023/05/Ley-31740-LPDerecho.pdf

Reaño Peschiera, J. L., & Medina Frisancho, J. L. (2023). *Criminal compliance* en el Perú: la necesidad de una reforma urgente y parcial al régimen de responsabilidad penal corporativa. *Themis*, (83), 159–175. https://doi.org/10.18800/themis.202302.020

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril del 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial de la Unión Europea, L 119/1. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679