Integración normativa para la gestión de riesgos sobre sistemas de información empresarial

Liliana Vaudo*
RVLJ, ISSN 2343-5925, ISSN-e 2791-3317, N.º 21, 2023, pp. 151-173.

Sumario

Introducción

No se puede pensar hoy día en la aplicabilidad de controles vinculados a la gestión de riesgos de la información enfocados únicamente en empresas de tecnología, tales como las empresas Fintech, sino que los avances tecnológicos y el uso de tecnología en la comunicación, prestación de servicios, gestión de información sobre clientes o en la nube, nos enfrentan cada día a nuevos retos.

Los estándares internacionales ofrecen regulaciones que plantean mecanismos de prevención de riesgos en la seguridad de la información, no siendo suficientes las normas constitutivas de las compañías, sino que las mismas

* **Universidad Central de Venezuela** (Caracas-Venezuela), Abogado, Especialista en Derecho Procesal, Especialista en Ciencias Penales y Criminológicas, Doctora en Ciencias mención «Derecho». **Universidad Metropolitana** (Caracas-Venezuela), Profesora Titular-Investigador. lvaudo@unimet.edu.ve, Orcid 0000-0002-6008-2066.

cuenten con manuales que recojan las políticas de cumplimiento de deberes asumidos conforme a las características de su labor y su naturaleza.

Igualmente, requieren contar con códigos de ética que reflejen los valores, principios, misión y visión de la organización. Ello, con la finalidad de una sana convivencia en las relaciones institucionales, laborales, de vigilancia que establezcan parámetros mínimos de conducta, operatividad, respeto a los derechos humanos y el modo en el cual se va a designar a los órganos de cumplimiento normativo y su responsabilidad en la gestión y vigilancia. Con relación a la seguridad y protección de data, se busca la lealtad y fidelidad dentro de la organización, respecto al funcionamiento y la prohibición de revelación de información confidencial.

Con base en este preámbulo se propone indagar respecto a cuáles políticas de cumplimiento pueden seguir las empresas para la protección y seguridad de la información, a través de las cuales se establezcan lineamientos basados en estándares nacionales e internacionales, de cómo se almacenan y transmiten datos a través de diferentes mecanismos. Estas políticas deberán entenderse de obligatorio cumplimiento por parte de todos los grupos de interés.

La relevancia deriva de que hoy día las empresas emplean plataformas tecnológicas en sus operaciones, pagos a proveedores, pagos a trabajadores, por lo cual habrá un especial interés en la protección de la confidencialidad y seguridad de la información, así como de la licitud de las actividades.

Algunos organismos han emitido normas de estandarización internacional, con el fin de implementar políticas preventivas a fin de mejorar las condiciones de vida y bienestar de las sociedades para el logro de un desarrollo económico sostenible, destacando la Organización Internacional de Normalización, a través de las Normas International Organization for Standardization (ISO).

En este sentido, se procederá a revisar cuáles de esas normas y de las disposiciones del ordenamiento jurídico venezolano contienen estándares que aporten a la gestión de riesgos empresariales, protegiendo la reputación

empresarial y el logro de un buen gobierno corporativo. Igualmente, se revisará la normativa y recomendaciones de los entes reguladores y fiscalizadores en distintos sectores, como el bancario, valores, criptomonedas y sector asegurador, destinadas a garantizar el correcto funcionamiento de los sistemas de tutela de la información y comunicación.

Todos estos aspectos van dirigidos a buscar la mejor manera de evitar y solventar la responsabilidad por fallas de operación o en la gestión de riesgos ante problemas operacionales que interrumpan el servicio o causen daño a clientes y usuarios.

En cuanto al métodos y objetivos, se emplea el método de investigación documental descriptivo y exploratorio, con ocasión de la obtención de datos derivados de la revisión de la normativa internacional sobre estándares de cumplimiento, como las normas del Grupo de Acción Financiera del Caribe (Gafic) los Objetivos de Desarrollo Sostenible de las Naciones Unidas y las Normas de Estandarización, así como las normas del Derecho positivo venezolano y algunos textos de autores que tratan temas vinculados con la buena gobernanza organizacional. Para Baena Paz, este método de investigación consiste en la «búsqueda de una respuesta específica a partir de la técnica de selección y recopilación de información y materiales bibliográficos»[1], en tanto que Tancara indica que se trata de un análisis predominantemente cualitativo, sobre fuentes bibliográficas teóricas[2].

Se plantea como objetivo general conocer las políticas de cumplimiento corporativo que debe implementar una empresa venezolana para gestionar los riesgos informáticos, que incluye: i. revisar las normas de estandarización internacional y las normas regulatorias emanadas de los entes administrativos, relacionadas con la seguridad de la información; ii. determinar el modo en el cual se debe involucrar a los grupos de interés dentro de la empresa en los

1 Baena Paz, Guillermina: *Metodología de la investigación.* Grupo Editorial Patria. México, D. F., 2014, p. 12.

2 Tancara, Constantino: *La investigación documental en la investigación científica*. Centro Nacional de Documentación Científica y Tecnológica. La Paz, 1988, pp. 6-9.

procesos de elaboración y seguimiento de dichas políticas de cumplimiento y de responsabilidad empresarial; iii. establecer el modo de integrar las políticas de seguridad informática en los programas de *compliance* empresarial.

Se busca dar respuesta a las siguientes preguntas: ¿cuál es el alcance de la normativa de estandarización internacional y las normas emanadas de los entes fiscalizadores? y ¿qué debe hacer una empresa para garantizar la ciberseguridad en las políticas de *compliance* corporativo?

1. Gestión de la información empresarial

Hablar de ciberseguridad es una labor necesaria en toda organización, debido a que la tecnología está presente en cada proceso que esta realiza, facilitando el intercambio de información y el desarrollo de las actividades, que ofrece soluciones tanto a la empresa como a la colectividad.

Para garantizar la implementación de programas de *compliance*, debe considerarse la protección de datos y seguridad en la información. En tal sentido, toda la serie de normas ISO 27000, dictadas por la Organización Internacional de Normalización, va dirigida a la protección de la información empresarial, incluyendo los controles y procedimientos de seguridad relacionados con la adquisición de productos técnicos.

Para ello, la norma ISO 27001 contempla el Sistema de Gestión de la Seguridad de la Información (SGSI), contra toda amenaza que pueda afectar el desarrollo y la continuidad de las actividades organizacionales. Su implementación persigue preservar la confidencialidad, la integridad y la disponibilidad de la información, definiendo la política, su alcance, análisis y gestión de riesgos e implementación, controles, declaración de aplicabilidad, así como medidas de prevención y correctivas.

La correcta gestión de riesgos es la que determinará el alcance de la norma y su aplicabilidad, así como las medidas apropiadas para prevenir y contrarrestar posibles daños, siguiendo como pasos: i. Identificar los activos informáticos que aportan valor a la empresa, los equipos, el capital humano, las ideas

y proyectos, las patentes, marcas, obras de creación intelectual. ii. Establecer los aspectos vulnerables que indican debilidades y hacen susceptible al activo de sufrir daños. iii. Ver cuáles son las amenazas que puedan dañar a los activos informáticos de la organización, como hackeos o espionaje. iv. Aspectos legales que debe cumplir la empresa con sus socios, trabajadores y proveedores. v. Identificación de posibles riesgos para cada activo, su disponibilidad y confidencialidad, a fin de realizar el cálculo de este con base en probabilidades de que se produzca. vi. Identificación del riesgo procediendo a asumirlo, reducirlo y eliminarlo.

Relacionado con lo anterior, la norma ISO 27002 establece una serie de políticas para la seguridad de la información destinadas al control de riesgos, incluyendo actividades como el uso de dispositivos celulares, el teletrabajo, elección en la contratación de recursos humanos, inventario de los activos.

Trata además, en su capítulo 9, del control sobre el acceso digital a la información, nube, gestión de contraseñas, protección de la información de los clientes, información sobre salud física o mental de trabajadores y usuarios, seguridad laboral y ambiental, creación de *backups* para respaldo de la información, programas antivirus, *spam* y *malwares.*

La relevancia de la protección de datos está reseñada en el Reglamento de la Unión Europea 2016/679[3], considerando que se trata de un derecho que debe valorarse en equilibrio con otros derechos fundamentales, tales como el respeto a la vida privada y familiar. En tal sentido, indica el Reglamento que:

> El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios

[3] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27-04-16, considerando 4, www.boe.es.

> reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística.

Todo lo anteriormente mencionado debe ir apoyado por una permanente comunicación con los grupos de interés con el fin de prevenir que sean objeto de procederes malintencionados y fraudulentos; igualmente a la protección de mensajerías, acuerdos de confidencialidad y sistemas operativos.

La norma ISO 27002, de igual manera, recomienda establecer límites en el acceso a la información de la empresa por parte de colaboradores y proveedores (ver más en capítulo 15) y la debida gestión de incidentes que surjan y modo de atenderlos o resolverlos sin interrumpir las actividades (ver capítulo 17).

Los beneficios que aporta el atender a este estándar internacional incluye mejoras económicas, prevención de riesgos y responsabilidad empresarial, optimización en los procesos, participación en estos, aumento de la productividad y a la buena reputación organizacional.

2. Empresas de tecnología financiera

Es importante definir lo que se entiende por empresas de tecnología financiera (Fintech). En este sentido, el Banco Interamericano de Desarrollo indica que las empresas Fintech son empresas proveedoras de productos y servicios financieros innovadores mediante el uso de tecnologías que desafían el sistema financiero tradicional y sus modelos de negocios, pero augura un profundo cambio en los mercados financieros. Este informe lo elabora conjuntamente con Finnovista, organización que realiza actividades de *networks*, eventos y programas vinculados con Fintech para lograr la transformación de servicios financieros[4].

[4] Banco Interamericano de Desarrollo (BID) y Finnovista: *Fintech: Innovaciones que no sabías que eran de América Latina y el Caribe*. Mayo 2017, http://dx.doi.org/10.18235/0000703.

Existe una variedad de ámbitos normativos en el tema de la tecnología financiera, existiendo, entre otras regulaciones, las vinculadas con los sectores financiero, asegurador, mercado de valores y criptomonedas.

2.1. Tecnología financiera bancaria

El ordenamiento jurídico venezolano entiende por empresas Fintech del sector bancario, según la Resolución N.º 001-21:

> Instituciones de Tecnología Financiera del Sector Bancario (ITFB): Toda persona jurídica de carácter público o privado, nacional o extranjera, autorizada por la Sudeban para prestar en el país los servicios financieros contemplados en la presente normativa, a través del uso de nuevas tecnologías[5].

Dicha normativa está destinada a regular servicios tecnológicos que garanticen la seguridad de las operaciones y de la información de los usuarios, mediante la incorporación de servicios financieros mediados por la tecnología que facilitan las operaciones de intermediación financiera.

Haciendo un paréntesis, es importante señalar que Abache –citando a Fraga-Pitalluga–, sostiene la existencia de usurpación de funciones del Poder Legislativo, por parte de la Sudeban cuando emite la Resolución N.º 001-21, toda vez que tanto la regulación sobre la constitución, requisitos de las empresas Fintech, como las autorizaciones operativas de las ITFB son materia de reserva legal. En concreto indica:

> Esta forma de incompetencia se produce cuando la Administración dicta actos administrativos, de efectos generales o particulares, en materias que solo pueden ser reguladas por el legislador. Este vicio se producirá,

[5] Resolución N.º 001-21, sobre Normas que Regulan los Servicios de Tecnología Financiera (Fintech), Sudeban, *Gaceta Oficial de la República Bolivariana de Venezuela* N.º 42 151, de 17-06-21, artículo 1.

> en consecuencia, cada vez que la Administración irrespete el principio de la reserva legal que rija en una materia determinada[6].

En tal sentido, sería competencia del ente administrativo regular las actividades económicas de sociedades mercantiles del sector bancario, que abarca instituciones que realicen actividades de intermediación financiera, casas de cambio y fondos de garantías, entre otros operadores bancarios. De manera que, como indica Abache, únicamente la Asamblea Nacional puede restringir el derecho a la libertad económica y resulta evidente que a través de la referida norma sublegal, se limita la operación de las Instituciones de Tecnología Financiera del Sector Bancario (ITFB) restringiendo su libertad de empresa[7]. Todo esto se vincula con lo dispuesto en el artículo 136 de la Constitución, que establece:

> El Poder Público se distribuye entre el Poder Municipal, el Poder Estadal y el Poder Nacional. El Poder Público Nacional se divide en Legislativo, Ejecutivo, Judicial, Ciudadano y Electoral. Cada una de las ramas del Poder Público tiene sus funciones propias, pero los órganos a los que incumbe su ejercicio colaborarán entre sí en la realización de los fines del Estado[8].

También define la Resolución N.º 001-21, lo que se entiende por «tecnología financiera», indicando que son: «Soluciones financieras propiciadas por la tecnología, que involucra a todas aquellas empresas de servicios financieros que utilizan procesos y sistemas tecnológicos de avanzada para poder ofrecer productos y servicios financieros innovadores bajo nuevos modelos de negocio» (artículo 1).

Igualmente se extiende a las denominadas *Startups*, que son aquellas que poseen un modelo de negocio que emplea tecnología, ya sea *blockchain*, *big data*,

---

6 Abache, Serviliano: «La regulación de las "Fintech" en Venezuela». En: *Revista de la Facultad de Derecho*. N.º 75. UCAB. Caracas, 2021, p. 116.

7 Ibíd., p. 117.

8 *Gaceta Oficial de la República Bolivariana de Venezuela* N.º 36 860, de 30-12-99.

redes inalámbricas, inteligencia artificial, la nube, ya sea como proveedores de servicios de pago. Estos últimos deben igualmente registrarse y presentar sus estados económicos, pero al Banco Central de Venezuela, y reportar actividades sospechosas ante el Órgano Superior de Inteligencia Financiera.

Las empresas de Tecnología Financiera del Sector Bancario (ITFB), conforme al artículo 16 de la Resolución N.º 001-21, únicamente podrán incluir como objeto social los servicios constituidos por:

> Productos dentro de las instituciones bancarias.
>
> Productos de pago y almacenamiento de dinero.
>
> Nuevos modelos de negocios vinculados con las instituciones financieras.

Deben constituirse como compañía anónima y con no menos de 5 socios, estar domiciliadas en Venezuela y prestar una fianza de fiel cumplimiento no menor a veinte mil euros (€20 000,ºº) conforme al tipo de cambio determinado por el Banco Central de Venezuela, expedidas por alguna institución bancaria o aseguradora, con el fin de garantizar su funcionamiento. De igual manera deberán solicitar autorización para funcionar a la Superintendencia y una vez otorgada, contará con 120 días para comenzar a operar.

La Resolución N.º 001-21 exige además que los modelos de contratos sean aprobados por la Superintendencia y, en caso de desear no continuar funcionando, solamente podrán hacerlo a partir de los 90 días siguientes a la autorización dada por la Superintendencia. Con relación a las obligaciones que deben asumir las empresas Fintech del sector bancario, el artículo 24 de la Resolución N.º 001-21, le impone las siguientes:

> Realizar actividades de monitoreo permanente.
>
> Disponibilidad de los servicios prestados a los clientes.
>
> Llevar el registro cronológico de las transacciones efectuadas a través de su plataforma tecnológica, que permita identificar origen y destino de los fondos, fecha, hora, dirección IP y usuario.

Elaborar planes de contingencias tecnológicas que permitan en todo momento la continuidad de las operaciones soportadas en la plataforma tecnológica, frente a posibles interrupciones graves del servicio.

Establecer mecanismos de evaluación, gestión y mitigación de los riesgos tanto implícitos como eventuales.

También deben cumplir con exigencias en el ámbito de las auditorías, las cuales deben realizarse de manera transparente por auditores externos e independientes, debiendo seguir los criterios de contabilidad que son aplicables a las Casas de Cambio.

2.2. Mercado de valores

Hoy día todo tipo de negocio puede realizarse en los mercados financieros y bursátiles a gran velocidad, pudiendo obtener información de las tendencias del mercado de manera inmediata y saber si conviene o no intercambiar valores, pudiendo obtener beneficios ventajosos de manera inmediata. Muchos de los procesos se realizan empleando inteligencia artificial que permite aumentar las operaciones y sus montos.

El uso de cadenas de bloques (*blockchain*) cifradas permite realizar transacciones mediante un registro único, eliminando los intermediarios y protegiendo las operaciones, pero no todas las inversiones monetarias digitales se realizan con este nivel de seguridad, requiriendo su protección.

La Superintendencia Nacional de Mercado de Valores (Sunaval), en el año 2021, dictó una serie de disposiciones dirigidas al sector bursátil, para prevenir la legitimación de capitales, el financiamiento de la proliferación de armas de destrucción masiva y el terrorismo, incluyendo a las empresas Fintech de este sector, a través de la Circular N.º 00009, sobre «Normas de Buen Gobierno Corporativo», aplicables a empresas de tecnología financiera vinculadas con el sector bursátil[9].

[9] Circular N.º 00009, de 30-11-21.

Destacan, de igual modo, la Providencia N.º 001, sobre «Normas relativas al Buen Gobierno Corporativo del Mercado de Valores»[10], que insta a los *stakeholders* (accionistas, junta directiva, gerencia, empleados, proveedores, clientes, reguladores y comunidad) a tutelar y vigilar las prácticas vinculadas a las políticas de gestión establecidas en la Ley del Mercado de Valores, gestión integral de riesgos, fiscalización y administración de delitos, como la legitimación de capitales, el desarrollo de programas de formación y capacitación (artículo 40).

Por otra parte, se encuentra la Providencia N.º 209-2021, sobre «Normas de Administración y Fiscalización de Riesgos»[11], destinada a la prevención de la legitimación de capitales, el financiamiento del terrorismo y la proliferación de armas de destrucción masiva (artículos 6-8). Esta normativa contempla las medidas que deben incorporar los sujetos obligados que incluyen la debida diligencia.

El Oficial del cumplimiento será el órgano encargado de garantizar su observancia. Estas disposiciones se basan en las Recomendaciones del Grupo de Acción Financiera Internacional (Gafi) persiguiendo la lucha contra los delitos financieros con un enfoque basado en riesgos (recomendación 1)[12].

En general, el sector bursátil se rige por el Decreto-Ley de Mercado de Valores[13], que contempla algunas regulaciones sancionatorias ante la inobservancia o cualquier violación del Decreto-Ley, sus reglamentos, circulares y demás disposiciones emanadas por Sunaval, que no tengan sanción específica y que no haya afectado los intereses o afectado los derechos de los inversionistas, será sancionado con multa de mil a cinco mil U. T. (artículo 129).

---

10 *Vid*. *Gaceta Oficial de la República Bolivariana de Venezuela* N.º 42 171, de 19-07-21.

11 *Vid*. Ídem.

12 *Vid*. *40 recomendaciones del Gafi*, actualizadas octubre 2020, www.cfatf-gafic.org.

13 *Vid*. *Gaceta Oficial de la República Bolivariana de Venezuela* N.º 6211 extraordinario, de 30-12-15.

2.3. Mercado asegurador

Las empresas aseguradoras en Venezuela cuentan con normas de rango sublegal respecto a riesgos de legitimación de capitales, financiamiento del terrorismo y de la proliferación de armas de destrucción masiva[14].

También cuentan con un sistema en línea a través de la Superintendencia de la Actividad Aseguradora (Sudeaseg), en la cual las empresas del sector reportan tanto la «declaración de origen de los fondos» como la declaración de encontrarse en el ejercicio de la actividad por la cual fueron autorizados. Es decir, que estos procesos se realizan a través de sistemas de tecnología.

3. Ética, autorregulación y responsabilidad empresarial

El modo como se lleva a cabo la gestión de gobernanza corporativa por parte de su consejo de administración, junto al cuerpo de cumplimiento, los órganos de auditoría y el control de todos los sectores que hacen vida en la organización, debe ir de la mano con la incorporación de personal resiliente a los cambios sociales, políticos, económicos y tecnológicos, especialmente frente a los embates de la crisis eléctrica y de internet que obligan a buscar nuevas fuentes generadoras que no dañen el entorno.

En Venezuela, Rodríguez Morales se fundamenta en los estándares de cumplimiento internacionales aportados por la Organización Internacional de Normalización (ISO), que sustituye a la Norma 19600[15], expresando que el

---

[14] *Vid*. Sudeaseg, Providencia N.º SAA-8-004-2021, sobre Normas relativas a la fiscalización y administración de riesgos sobre legitimación de capitales, financiamiento del terrorismo y proliferación de armas de destrucción masiva aplicables a los sujetos obligados al control de la Ley que rige la actividad aseguradora, *Gaceta Oficial de la República Bolivariana de Venezuela* N.º 42 128, de 17-05-21.

[15] *Vid*. Norma ISO 19600 (2016), ampliada en 2022 por la Norma ISO 37301 sobre *compliance*, igualmente relacionada con la Norma ISO 31301 sobre gestión de riesgos y Norma ISO 37002 sobre creación de canales de denuncia. www.iso.org.

cumplimiento normativo, también denominado *compliance*, no es más que «la observancia de todas las obligaciones que la organización debe cumplir»[16].

En tanto que Kuhlen indica que el *compliance* es un conjunto de «medidas de prevención a través de las cuales las empresas pretenden asegurar tanto el cumplimiento de las normas aplicables a la misma y a sus trabajadores, como la denuncia y eventual sanción de esta»[17].

En los criterios de sostenibilidad deberá considerarse:

> a. Que el uso de tecnología esté vinculado con el empleo de energías verdes o políticas circulares.
>
> b. Que en el aspecto social se atienda las necesidades de la colectividad y la protección de su información, así como la de sus trabajadores, a través de: i. la protección de la igualdad al acceso a la tecnología sin importar el género, raza, condición, edad, religión o preferencias políticas; ii. desarrollo de nuevos proyectos con empleo de tecnologías en pro de las comunidades y del sistema económico; iii. solución de conflictos empleando la tecnología digital para favorecer la celeridad y protección de identidad; iv. los supervisores deben proveer oportunidades para capacitación y desarrollo.
>
> c. En el ámbito de la gobernanza organizacional, se debe motivar el uso de la tecnología con criterios éticos para prevenir cualquier forma de corrupción, financiamiento de actividades de delincuencia organizada, implementando sanciones disciplinarias para cualquier forma de uso de la tecnología contrario al deber de sigilo, debiendo tutelar la propiedad intelectual.

Por su parte, la Resolución N.º 083-18, emanada de la Superintendencia Nacional de Instituciones del Sector Bancario[18], establece el deber de elaborar

---

[16] Rodríguez Morales, Alejandro: *Criminal* Compliance. *Cumplimiento normativo penal y Derecho Penal Económico.* Ediciones Paredes. Caracas, 2021, p. 23.

[17] Kuhlen, Lothar: Compliance *y teoría del Derecho Penal*. Marcial Pons, Madrid, 2013, p. 52.

[18] Sobre Normas relativas a la administración y fiscalización de los riesgos relacionados con la legitimación de capitales, financiamiento al terrorismo y financiamiento

manuales de cumplimiento que contemplen todos los aspectos vinculados con la prevención y atención de los riesgos de delitos de legitimación de capitales, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva, entre los que exige la elaboración de un Código de Ética (artículo 37).

En tal sentido, Vázquez-Parra *et al*. sostienen que resulta fundamental para las organizaciones contar con normas éticas que incorporen valores y principios, visión y misión de la empresa, incluyendo lo atinente a transparencia, solidaridad, igualdad, el respeto y protección de la data y privacidad en el manejo de la información, evitando cualquier acto que implique deslealtad competitiva[19].

Este correcto modo de proceder, sellando un compromiso entre los sectores de interés conformados por los socios, clientes, trabajadores, administradores, gerentes y oficiales de cumplimiento, se consolida en la realización de actividades económicas sostenibles que produzcan confianza para los usuarios, en especial cuando las mismas se realizan por medio de la tecnología, como se ha señalado en otra oportunidad: constituyen la base del logro del éxito empresarial, ya que será preferida por los usuarios, debido a su prestigio al garantizar que los procesos productivos se desarrollan respetando la sana competencia y la valoración de los principios económicos contenidos en la Constitución[20].

En todo caso, debe evitarse cualquier conducta comprometedora que pueda perjudicar la reputación empresarial como el deber de no aceptar dádivas con

---

de la proliferación de armas de destrucción masiva aplicables a las instituciones del sector bancario, *Gaceta Oficial de la República Bolivariana de Venezuela* N.º 41 566, de 17-01-19.

19 Vázquez-Parra, José Carlos *et al*.: «*Labor Inclusion with a Gender Perspective in Complex Environments: Firm Steps for the Post-Pandemic Economic Recovery*». En: *The International Journal of Organizational Diversity*. Vol. 23 (1). 2023, pp. 94-97.

20 Vaudo, Liliana: «*Compliance* corporativo como política de prevención de actos que perjudican la reputación organizacional». En: *Revista Venezolana de Derecho Mercantil*. N.º 8. Sovedem. Caracas, 2022, p. 166, www.sovedem.com.

ocasión de los deberes laborales que son contrarias a la ética, ni otro tipo de conducta no cónsona, como desempeñar las actividades bajo efecto de sustancias prohibidas aun si se tratare de aquellas faenas que se realizan mediante plataformas digitales, ya que pueden perjudicar la seguridad informática.

Refuerza este aspecto Sanclemente-Arciniegas, quien afirma que el *compliance* es una nueva rama del Derecho vinculada al combate de la corrupción dentro de las empresas; y afirma que: «los postulados de esa nueva disciplina son especialmente pertinentes en materia de lucha contra la corrupción, pues es en ese ámbito donde se manifiesta con más claridad la intención de erigir al poder económico privado como un agente al servicio de la protección del interés general»[21].

Para este tipo de conducta aplica la norma positiva penal, una serie de penas sobre diferentes órganos dentro de las instituciones financieras, de mercado de valores y en el sector asegurador sobre sujetos activos que ejercen funciones gerenciales, administrativas y otros altos cargos. Por esta razón, es importante que los grupos de interés interno se identifiquen con la misión, la visión, los valores y principios de la empresa, debiendo comprometerse a cumplir tanto la norma positiva como las de Derecho blando, debiendo los cuerpos de cumplimiento normativo realizar los ajustes que requiera esa implementación y tomar en consideración las observaciones y recomendaciones de los entes reguladores. Así, el Decreto-Ley de Instituciones del Sector Bancario dispone:

> Las instituciones del sector bancario, así como las personas naturales que ocupen en ellas cargos de administración o de dirección, consejeros o consejeras, asesores o asesoras, consultores o consultoras, auditores internos y externos, gerentes de áreas, secretarios o secretarias de la junta directiva o cargos similares, de hecho o de derecho, que infrinjan el presente Decreto con rango, valor y fuerza de Ley, y todo el cuerpo

[21] Sanclemente-Arciniegas, Javier: «*Compliance*, empresas y corrupción, una mirada internacional». En: *Derecho PUCP*. N.º 85. Pontificia Universidad Católica del Perú. Lima, 2020, p. 10, doi.org/10.18800/derechopucp.202002.001.

> normativo emitido por la Superintendencia de las Instituciones del Sector Bancario, incurrirán en responsabilidad administrativa sancionable con arreglo a lo dispuesto en el presente título (artículo 185)[22].

Las normas sancionatorias previstas en el título VII del Decreto-Ley establecen un régimen sancionatorio especial sobre las personas naturales que ocupen los cargos descritos y las penas pueden alcanzar hasta 15 años de prisión, más 15 años de inhabilitación posterior al cumplimiento de la pena corporal (artículos 212-217, 221 y 228). También se aplican sanciones a los funcionarios de la Superintendencia de las Instituciones del Sector Bancario y del Fondo de Protección Social de los Depósitos Bancarios, y las personas naturales o jurídicas que estos designen para ser administrador o junta administradora e incurran en delitos aprovechando su cualidad.

También contempla el Decreto-Ley antes mencionado, el delito de «fraude electrónico», estableciendo en su artículo 224:

> Quien, a través de la manipulación informática o mecanismo similar, con ánimo de lucro, efectúe una transferencia o encomienda electrónica de bienes no consentida, en perjuicio de la institución del sector bancario o de un usuario o usuaria, será penado con prisión de ocho a diez años.
>
> Con la misma pena serán castigadas las personas naturales identificadas en el artículo 185 del presente Decreto con rango, valor y fuerza de Ley, o los empleados de la institución del sector bancario que colaboren en la comisión de las transferencias antes mencionadas.

La sanción viene justificada porque las empresas, en su libertad para realizar las actividades económicas, deben ajustar su conducta tanto a la norma jurídica como a sus normas internas, asumiendo responsabilidad para el caso de su incumplimiento, ya que el objeto de las normas de internas se basa en la debida diligencia y prevención de ilícitos de distinta índole.

---

[22] *Vid*. *Gaceta Oficial de la República Bolivariana de Venezuela* N.º 40 557, de 08-12-14.

3.1. Seguridad y protección de datos tecnológicos

Cualquier organización que incorpore la tecnología en sus procesos, y muy especialmente las empresas de tecnología financiera, que funcionan en entornos digitales, requieren especiales exigencias en su marco regulatorio. Por tal razón, luego de la revisión de las normas de estandarización y las regulaciones nacionales, se puede resumir como aspectos a ser enfocados:

Preservación de los documentos, facturas y toda la información por no menos de cinco años.

Los datos deben ser fidedignos para reflejar la verdadera situación de la empresa y de los clientes.

Debe revisarse y confrontarse la información en un proceso integrador de todas las fuentes.

Debe manejarse de manera confidencial.

Garantizar la seguridad de los sistemas, evitando cualquier alteración fraudulenta de los datos.

Establecer los canales de denuncia seguros y confidenciales frente a adulteración o uso indebido de la información

Orientar a los empleados y usuarios sobre no compartir claves ni información, generando copias de seguridad, frente a posible intrusión de *hackers.*

Hacerse responsable por errores o daños derivados de fallas tecnológicas.

Encriptación de la información.

Uso de plataformas tecnológicas privadas (VPN) que contengan herramientas de fácil implementación.

Reportar actividades sospechosas al Oficial o cuerpo encargado del *compliance.*

Incorporar nuevos elementos de seguridad como reconocimientos faciales, códigos QR, sistemas de *blockchain* para prevenir actividades que causen daño o pongan en peligro de la información.

Estas exigencias implican la necesaria contratación de personal con conocimientos en el área y que sirvan de multiplicadores a los restantes miembros de la organización, generando confianza y conciencia sobre la importancia de preservar la ciberseguridad. Para ello, se debe designar un cuerpo de cumplimiento encabezado por el Oficial de cumplimiento, quien deberá organizar una comisión de *compliance* multidisciplinaria, dentro de la cual necesariamente debe haber expertos en el área de protección de datos, así como abogados que contribuyan a la elaboración de las normas regulatorias internas. Algunas funciones de este cuerpo serían:

> Velar por la correcta implementación de las políticas de cumplimiento.
>
> Impartir el obligatorio adiestramiento del personal sobre la gestión de riesgos, ética y protección de datos, así como la importancia de hacer seguimiento y denunciar las conductas que atenten contra la ética empresarial.
>
> Evaluar periódicamente la implementación de las políticas de *compliance* y gestión de riesgos vinculados a la tecnología de la información.
>
> Ejercer la tutela sobre la protección de datos e información confidencial y reportar las actividades sospechosas.

Para abordar este tipo de riesgos, la Organización Internacional de Normalización dictó la Norma ISO 27008[23], a través de la cual se busca:

> Establecer las deficiencias de los sistemas de gestión y aplicar correctivos y controles de seguridad de la información, incluyendo modificar las reglas de seguridad y controles técnicos.
>
> Elaborar una ruta de identificación de impactos, amenazas y vulnerabilidades de la seguridad de la información.
>
> Mejorar los mecanismos para mitigar riesgos en esta área.
>
> Corregir deficiencias de seguridad.

[23] *Vid*. Organización Internacional de Normalización y Comisión Electrotécnica Internacional, Norma ISO/IEC 27008 sobre Sistemas de Gestión de Seguridad Informática, 2011, www.pmg-ssi.com.

De este modo se pueden adaptar los mecanismos de control para ajustarlos de manera resiliente a nuevos retos, para lo cual se requiere el compromiso de los entes de cumplimiento para garantizar la seguridad de la información, lo cual permite dar respuesta a la pregunta de investigación acerca de: ¿cuál es el alcance de la normativa de estandarización internacional y las normas emanadas de los entes fiscalizadores?

3.2. Aplicabilidad de sanciones penales

Cuando la gestión de riesgos sobre sistemas informáticos traspasa los límites permitidos pueden producirse sanciones penales como consecuencia de estas conductas. En tal sentido, diversas leyes dentro del ordenamiento jurídico venezolano contemplan este tipo de ilícitos, tales como: la Ley especial sobre Delitos Informáticos, la Ley de Instituciones del Sector Bancario, la Ley de Propiedad Industrial o el Código Orgánico Tributario.

El Código Orgánico Tributario (artículos 118-124)[24] contempla como delito la divulgación de información, indicando que se considera delito y se castiga con prisión de 3 meses a 3 años:

> La divulgación o el uso personal o indebido de la información confidencial proporcionada por terceros independientes que afecte o pueda afectar su posición competitiva, por parte de los funcionarios o empleados públicos, sujetos pasivos y sus representantes, autoridades judiciales y cualquier otra persona que tuviese acceso a dicha información.

La Ley sobre Delitos Informáticos[25] busca sancionar los delitos que se cometan mediante el empleo de medios informáticos; son aquellos que son cometidos por *hackers*, *crackers*, *frackers* y piratas informáticos, respecto

---

[24] *Vid. Gaceta Oficial de la República Bolivariana de Venezuela* N.º 6507 extraordinario, de 30-01-22.
Nota bene: vale aclarar que la anterior reforma fue efectuada por la Asamblea Nacional Constituyente, la cual no se encuentra habilitada para legislar; su único propósito es efectuar un proyecto de Constitución, de allí su discutible constitucionalidad.

[25] *Vid. Gaceta Oficial de la República Bolivariana de Venezuela* N.º 37 313, de 30-10-01.

de información personal, organizacional, financiera, mediante actos fraudulentos capaces de vulnerar la seguridad de los sistemas tecnológicos. Esta Ley es muy amplia al contemplar como sujetos víctimas de estos delitos a quienes sufran abusos contra su dignidad, pérdidas económicas, extorsión, fraudes o estafas, sabotaje, acceso no autorizado, espionaje informático, hurto de información, daños a datos, entre otros.

En materia de mercado de valores, se impone sanción penal que va de 3 meses a 2 años de prisión quienes hayan usado una información privilegiada de manera fraudulenta, más inhabilitación para el ejercicio de cualquiera de las actividades durante el lapso de 1 hasta 5 años (artículo 146 del Decreto-Ley de Mercado de Valores).

En tanto que en el ámbito bancario se observa que obtiene relevancia el peligro de ejecución de conductas que generen desestabilización del sistema, en especial aquellas de las cuales derivan delitos, como el de legitimación de capitales, el financiamiento del terrorismo y el financiamiento de actividades relacionadas con la proliferación de armas de destrucción masiva como deriva de la Resolución N.º 083-18 sobre «Normas relativas a la administración y fiscalización de los riesgos relacionados con la legitimación de capitales, financiamiento al terrorismo y financiamiento de la proliferación de armas de destrucción masiva aplicables a las instituciones del sector bancario», contentiva de directrices en materia de buen gobierno corporativo. Estas disposiciones se imponen también a las empresas Fintech de tecnología financiera vinculadas a este sector.

En materia de tecnología financiera, también se dictan normas similares por la Superintendencia Nacional de Valores, a través de la Providencia N.° 209-21; igualmente, por la Superintendencia de la Actividad Aseguradora, a través de la Providencia N.º SAA-8-004-2021.

La finalidad de estas regulaciones será la de imponer directrices para evitar que se utilice la fachada de la institución financiera y las empresas de tecnología financiera (Fintech) con el objetivo de ocultar el origen, propósito

y destino de los capitales ilícitos, o para desviar fondos de cualquier naturaleza hacia el financiamiento de grupos o actividades terroristas o la proliferación de armas.

Todo lo anterior debe ir respaldado por la creación de un sistema de denuncias, que proteja la identidad del denunciante, con el objeto de permitir la transparencia en las investigaciones sobre actividades sospechosas que puedan afectar el sistema financiero y perjudicar la reputación organizacional.

En este mismo orden, la Resolución N.º 001-21, dictada por la Superintendencia Nacional de Instituciones del Sector Bancario, está destinada a asegurar servicios tecnológicos que garanticen la seguridad de las operaciones y de la información de los usuarios, mediante la incorporación de servicios financieros mediados por la tecnología que facilitan las operaciones de intermediación financiera. Este cuerpo normativo regula las operaciones, directrices, inspección, contratos, revocatorias de funcionamiento a empresas de tecnología financiera del sector bancario que operan en Venezuela y ofrecen servicios financieros vinculados con depósitos, pagos y otros productos digitales. De este modo se ratifica la relevancia del *compliance* como mecanismo de retorno de la inversión, que beneficia tanto la imagen como la sostenibilidad de la empresa.

Todo lo anterior permite dar respuesta a la pregunta de investigación sobre: ¿qué debe hacer una empresa para garantizar la ciberseguridad en las políticas de *compliance* corporativo?

Conclusiones

La mayor parte de las empresas del mercado actual utiliza tecnología dentro de sus procesos, auditorías, operatividad, información de proveedores, clientes, personal; siendo que algunas realizan sus actividades empleando como herramienta principal el uso de la tecnología, tal y como ocurre con las operaciones de las empresas de tecnología financiera.

Para garantizar la operatividad y seguridad de la información, es fundamental que la empresa cuente con un sistema de gestión de riesgos informáticos para evitar ser objeto de ataques cibernéticos o cualquier conducta indebida que ponga en peligro la información privilegiada, la confianza en la organización, produciendo daños que afecten las relaciones con los usuarios, proveedores y demás grupos de interés.

Para el logro de estos fines es importante observar las normas de estándar internacionales, debido a que no bastan las regulaciones del Derecho positivo nacional, sino que se requiere una sólida autorregulación, que comporte su elaboración y supervisión por parte de personal calificado en los entes de cumplimiento interno.

* * *

Resumen: La gestión de riesgos en el ámbito de la información y ciberseguridad empresarial impone la elaboración de normas y procedimientos para prevenir situaciones que puedan representar daños a los sistemas informáticos vinculados con la protección de data tanto en las operaciones como en la propia confidencialidad y fidelidad de la información y la comunicación. La propuesta que se plantea va dirigida a explorar y evaluar cualitativamente el ámbito regulatorio nacional e internacional que permita lograr cumplir con estándares de certificación que brinden seguridad en la prestación de servicios, gestión de información sobre clientes, información en la nube y otros procesos que llevan a cabo las empresas dentro de su gestión, por lo cual la investigación se llevó a cabo de manera documental descriptiva. A partir de la propuesta se busca generar la discusión respecto a cuáles políticas debe implementar toda empresa en el ámbito de gestión de la información, partiendo de los estándares internacionales y normas nacionales, para generar confianza y prevenir conductas que puedan acarrear sanciones

e ir innovando ante los nuevos retos tecnológicos. **Palabras clave**: gestión, riesgos, cumplimiento organizacional, prevención, daño, seguridad, informática, tecnología, información. Recibido: 30-06-23. Aprobado: 28-09-23.