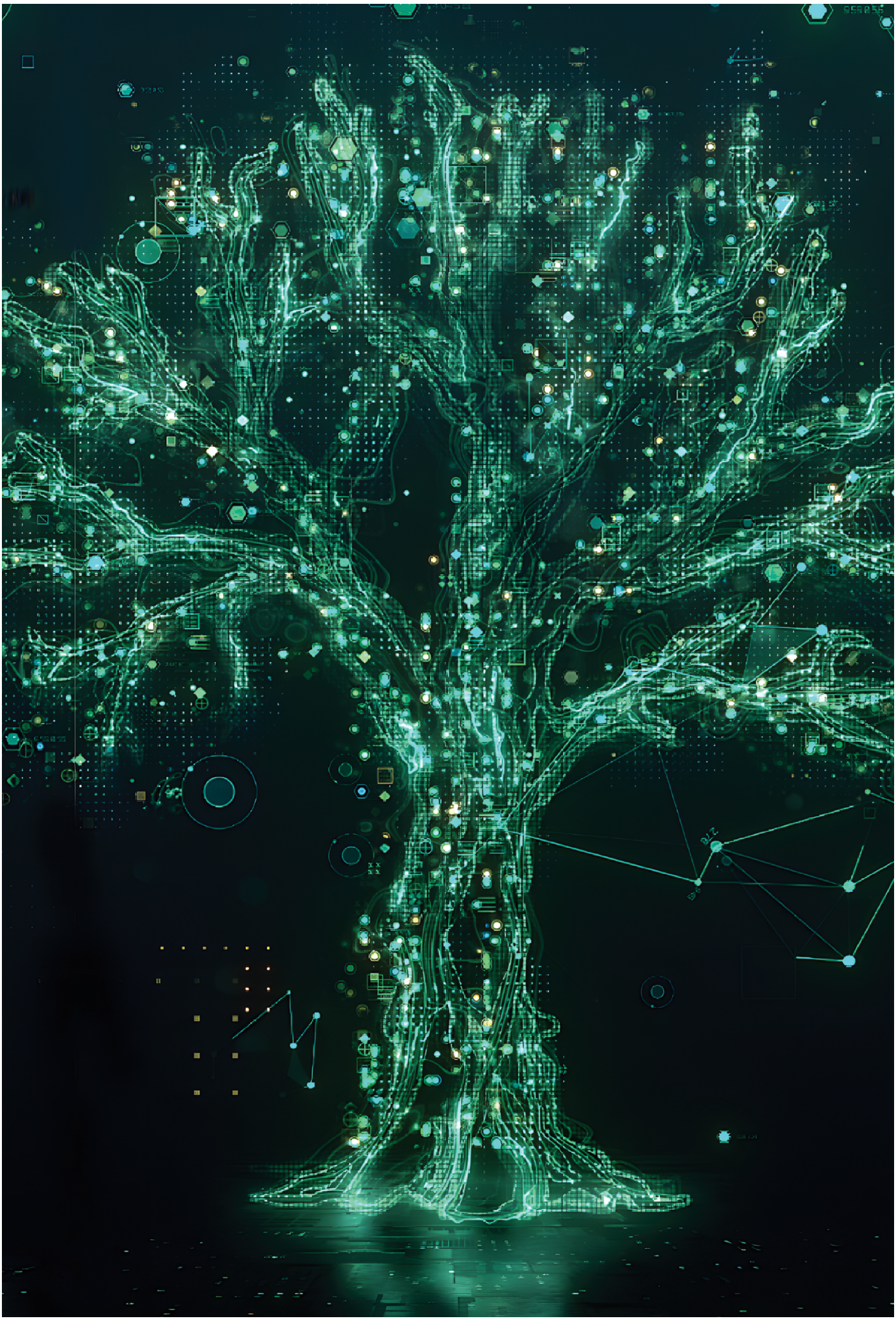
Deloitte.

Compliance*Trends*

by Deloitte

Edición 2

Índice



EDITORIAL

Tendencias reguladoras para un desarrollo sostenible

Manuel Gálvez | Socio Risk Advisory

La función de Ética y Cumplimiento día a día sigue posicionándose en el corazón estratégico de las organizaciones, esta acción no solamente se ve respaldada por el incremento de prácticas para generar confianza en los stakeholders con los que se interactúa, sino por el aumento de su participación en los diferentes procesos organizacionales a propósito de los nuevos cambios regulatorios nacionales e internacionales.

Con el objetivo de contribuir a las nuevas tendencias regulatorias y las mejores prácticas en Ética y Cumplimiento, en esta Segunda Edición de la Revista "Compliance Trends" hemos decidido incorporar temáticas asociados a los criterios Ambientales, Sociales y de Gobernanza ("ESG" según siglas en inglés) Gobierno de Datos, Proyecto de Ley sobre Fintech y Open Banking, Compliance en el ámbito de la protección de datos personales y a propósito de la Ley Nº 21.549 sobre Delitos Informáticos. Además, posicionar el rol de la función de Auditoría Interna y su agregación de valor, junto a la modernización de la función de Compliance de acuerdo con las nuevas tendencias globales.

Desde Deloitte confiamos en que el contenido de esta segunda edición de Compliance Trends sea el punto de partida para impulsar la discusión e integración de los diversos actores interesados dentro de la organización y que a su vez incentive el crecimiento sostenible para avanzar hacia el logro de los propósitos organizacionales bajo altos niveles de integridad y transparencia.


EUR/USD
2.3574
2.3585
9.7762

LEY FINTECH

La utilización de tecnologías para mejorar o automatizar servicios y procesos financieros

Por **José Tomás Lavín** | Director Deloitte Legal

Actualmente, y tras ser aprobado en general por amplia mayoría Congreso con fecha 12 de octubre del 2022, se encuentra en proceso de promulgación y públicación, el Proyecto de Ley que "Promueve la competencia e inclusión financiera a través de la innovación y tecnología en la prestación de servicios financieros" (Boletín N°14570-05), conocido también como "Ley Fintech".

Las denominadas Fintech corresponden a un sector integrado por empresas que utilizan la tecnología para mejorar o automatizar los servicios y procesos financieros.

Hoy, Chile no cuenta con un marco regulatorio vigente para estas actividades y, por tanto, se consideró al momento de presentar normativa , que era importante avanzar en regular el mercado de las denominadas empresas Fintech, de manera tal, de evitar los riesgos que produce la falta de regulación en la materia, tales como prácticas abusivas o lavado de activos. Adicionalmente, la normativa proyecto surge como una respuesta a nuevos modelos de negocio que se basan en el uso de tecnologías y digitalización de ciertos servicios financieros, los cuales aceleraron su expansión con motivo de la crisis sanitaria que aquejó a Chile y el mundo producto de la pandemia.

Lo más relevante de esta pronta ley es que viene a regular una serie de actividades financieras desarrolladas por Fintech que, en la actualidad debido a un vacío normativo derivado de la desactualización de la normativa aplicable, no se encuentran fiscalizadas por la Comisión para el Mercado Financiero (CMF). Dentro de las actividades contempladas en el proyecto de ley se encuentran: (a) las Plataformas de Financiamiento Colectivo; (b) los Mercados Secundarios y custodia de instrumentos financieros (dentro de lo que se encuentran comprendidas las criptomonedas); (c) la Intermediación y Enrutamiento de Órdenes; y (d) la Asesoría de Crédito y Asesoría de Inversión.

Un aspecto medular de la regulación es el de incorporar el concepto de “Finanzas Abiertas”, u “Open Banking”, según su terminología en inglés. Las Finanzas Abiertas operan en base al principio de intercambio de información financiera, mediante la cual los clientes voluntariamente entregan información para que pueda ser compartida entre distintas instituciones del rubro, con el fin de transparentar el mercado, estimular la competencia y disminuir las barreras de entrada. Esto se pretende realizar a través de interfaces de acceso remoto y automatizado que permitirán una interconexión y comunicación directa entre las instituciones financieras participantes del mercado. De esta forma, las Finanzas Abiertas traen como consecuencia, además de estimular la competencia, elevar los estándares en los que funciona la industria financiera, tanto para los nuevos actores como para los actores tradicionales.

En línea con lo anterior, es que entidades de alta relevancia, tales como, la Asociación de Bancos e Instituciones Financieras (ABIF) y FinteChile establecieron una mesa de trabajo con el objeto de establecer un sistema de Finanzas Abiertas. Fruto de lo anterior, en el mes de junio de este año, las referidas entidades firmaron un Acuerdo Marco, el cual es de carácter opcional, tanto para los bancos como para las Fintech. Este acuerdo, establece estándares de responsabilidad y seguridad, mecanismos de resolución, y protocolos de acceso que impulsarán el sistema de Finanzas Abiertas en el país. Los que deberán, por cierto, ser complementados con acuerdos bilaterales que establecerán las instituciones respectivas, con los aspectos específicos a considerar en la implementación de los acuerdos de lectura y procesamiento de datos.

Pareciera que la regulación avanza en la dirección correcta y acorde con el desarrollo tecnológico que ha acompañado el impulso de la industria Fintech. La ley, cuando sea promulgada y publicada, estimularía la competencia y el acceso al mercado financiero, sobre todo considerando que aun existe un porcentaje importante de la población que no tiene acceso al mercado financiero tradicional. Ejemplo significativo de ello, es el abrir el mercado de la intermediación financiera, el cual se encuentra actualmente restringido sólo a bancos, a través de sus filiales, y las corredoras de bolsa. Con esto, se abre la posibilidad de que las Fintech, cumpliendo con los requisitos establecidos en la Ley, también puedan prestar dicho servicio, ampliando de esta forma la competencia en el mercado de transacción de valores.

Por su lado, desde el punto de vista del acceso a financiamiento, al regular las denominadas "Plataformas de Financiamiento Colectivo", se norma una situación que actualmente ya opera, donde personas naturales ponen a disposición de las Fintech determinadas sumas de dinero, con la finalidad que éstas sean prestadas a otras personas, a cambio de un retorno por interés. La regulación de dicha actividad, junto con permitir el acceso a financiamiento a personas o PYMES que se encuentran fuera del acceso a crédito tradicional, viene a proteger tanto a acreedores como a deudores, evitando cualquier tipo de irregularidad o desprotección que puedan llegar a sufrir producto del vacío legal actualmente existente.

ESG

Sostenibilidad, Gobierno Corporativo y Compliance

Por **David Falcón** | Socio ESG

La discusión en torno a temáticas ambientales, sociales y de gobernanza (ESG por sus siglas en inglés) se ha arraigado en el sector empresarial a nivel mundial. Actualmente, estos criterios son abordados por múltiples actores: inversionistas, organismos gubernamentales, industrias, medios de comunicación, consumidores y los mismos empleados.

Habiendo cobrado tanta relevancia, es hoy una temática que las organizaciones, y sus respectivos Directorios, no pueden permitirse pasar por alto. Y es que además de las presiones por parte de los actores antes mencionados, ahora los reguladores financieros han irrumpido en escena.

A nivel global son varios los países que están incluyendo en sus regulaciones mtayores exigencias de divulgación de información ESG transitando de un mercado autorregulado con falta de reglas claras, a uno que promueva la transparencia, confianza y una mayor competitividad. La Comisión Europea, Inglaterra, Canadá y recientemente a nivel local, la Comisión para el Mercado Financiero (CMF) mediante la emisión de la Norma de Carácter General (NCG) 461, reflejan la relevancia que estas materias representan para la economía y la sociedad así como también, el deber de cumplimiento de las empresas y quiénes están a cargo de su gestión.

La razón que ha empujado a mirar en detalle las temáticas ESG por parte de los reguladores tiene directa relación con los potenciales efectos financieros que podrían derivar producto de la toma de decisiones que no incorporen estas temáticas toda vez que, una gestión deficiente en estas materias podría repercutir en los estados financieros de las compañías[1].

En este contexto, la normativa será aplicable a entidades supervisadas por la CMF tales como, bancos, compañías de seguros y emisores de valores de oferta pública, entre otros. El objetivo de la CMF es claro: que los inversionistas y el público en general puedan evaluar y seleccionar aquellas alternativas en que estarían mejor resguardados sus intereses y que de igual forma, puedan distinguir aquellas compañías más preparadas para identificar, cuantificar y gestionar sus riesgos en materia ESG. Para su correcta implementación, los requerimientos asociados a fortalecer el Gobierno Corporativo se ubican al centro de la Norma, estableciendo roles y funciones específicas para los directores[2].

Esto quiere decir que aquellas empresas que no han tenido

[1] Presentación CMF, "ESG y su importancia en la Regulación y el Gobierno Corporativo de las Empresas", Centro de Gobiernos Corporativos UC.

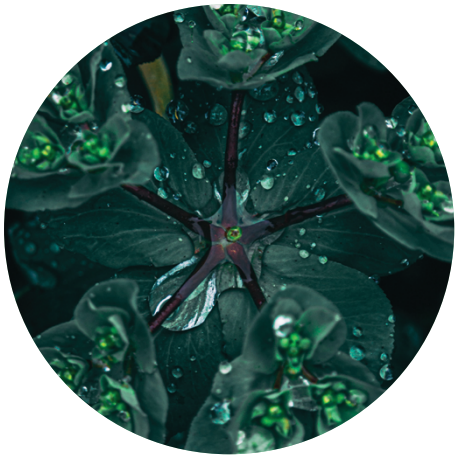
[2] Presentación Solange Berstein "Sostenibilidad y Supervisión: Divulgación de información al mercado financiero", Evento Deloitte, 2022

una gestión activa de la sostenibilidad deben ir preparándose desde ya, porque en el corto plazo deberán obligatoriamente transparentar su información y desempeño ESG de forma precisa, veraz y completa, es decir, con un sistema de compliance efectivo.

Siendo responsables de supervisar los riesgos y de administrar la creación de valor empresarial a largo plazo, los miembros del Directorio juegan un rol fundamental para evaluar y supervisar los impactos ambientales y sociales que tiene la entidad en su entorno. De igual modo, son responsables de comprender el impacto potencial y el riesgo relacionado a las temáticas ESG en el modelo operativo de la organización. Frente a esto, (y respondiendo a las preocupaciones de sus grupos de interés), las empresas están cambiando el paradigma que antiguamente se le otorgaba a la sostenibilidad, mejorando sus posturas y visión estratégica en materia ESG integrándolas de forma transversal en la estrategia corporativa. Lo cierto, es que desde que las temáticas ESG se han popularizado y han calado en la discusión, la tendencia ha impulsado a las organizaciones a perseguir prácticas sostenibles de largo plazo.

Puede ser desafiante para los Directorios lograr conectar temáticas tan globales, como lo son el cambio climático, la escasez hídrica o los derechos humanos, a las operaciones, estrategia y perfil de riesgo de una organización. Pero, dado que los factores ESG influencian y son influenciados por diversas áreas como sostenibilidad, operaciones, finanzas, riesgos, compliance, legal y recursos humanos, por nombrar algunas, los directores tienen un rol de liderazgo esencial que ejercer para impulsar y coordinar a sus equipos en el objetivo de generar valor de largo plazo, considerando a sus grupos de interés y a la sociedad en general.

Esto no es solo un asunto de relaciones públicas o de posicionamiento de marca – pese a que son consideraciones válidas–. Tampoco es solo un tema de prácticas éticas o tener un positivo impacto organizacional. Esto es también una cuestión de rentabilidad empresarial sostenida en el tiempo ya que las prácticas sostenibles tienen como objetivo asegurar que la organización genere valor y lo mantenga en el largo plazo.



Rol de Auditoría Interna respecto de los factores ESG (Enviromental, Social y Governance)

Por **Fernando Pino Santander** | Director Líder Internal Audit

No es necesario ser un experto en materias ambientales y sociales o especialista en regulaciones para darse cuenta de que la conciencia en materia de sostenibilidad de las organizaciones y la manera en que desarrollábamos los negocios han cambiado drásticamente.

Cada vez con mayor frecuencia, las empresas y la comunidad de negocio se encuentran impulsando sus operaciones con una alineación clara y directa hacia los factores Medioambientales, Sociales y de gobernanza, hoy, término acuñado en los aspectos de ESG (por sus siglas en ingles).

Estas materias se han posicionado con agilidad como uno de los temas a tratar por los Directorios y Alta Administración. De igual forma, ha movilizado a los reguladores a emitir normativas relacionadas que permitan disponer de información no financiera a inversionistas y grupos de interés, especialmente teniendo en consideración que la falta de gestión de estas temáticas puede tener efectos reales en rentabilidad y creación de valor corporativo.

Bajo este contexto, Auditoría Interna, quien de forma progresiva ha logrado una transversalidad en la organización, pareciese ser que es la llamada a llevar los controles internos apropiados, tomando un rol relevante para cuidar y agregar valor a la compañía frente a estos cambios y desafíos de los negocios en los tiempos actuales. Estos desafíos pueden ser vistos desde su participación más tradicional de aseguramiento de procesos ya definidos en esta materia o, pueden ser requeridos desde un foco consultivo como asesor de confianza del Directorio y la alta administración.

Teniendo en cuenta la normativa vigente emitida el año 2021 por la Comisión para el Mercado Financiero; NCG 461 sobre divulgación de información ESG, y los plazos establecidos para dar cumplimiento, la estrategia de la Auditoría Interna se ha robustecido para complementar la revisión de controles internos, así como también, materias emergentes necesarias, entre ellas ESG, Cyber, riesgos operacionales, entre otros.

Pensando en esta estrategia, es donde existen diversos focos de atención que deben ser considerados. Desde ámbitos normativos, calidad y consistencia de la información que sustentará el desempeño de la organización y la definición de responsabilidad operacional en la articulación del modelo, hasta las responsabilidades de la Alta Administración para la ejecución de los controles a nivel de entidad definidos para la aprobación del proceso.

Actualmente, muchas organizaciones funcionan con un grado de madurez distinto con reportes individuales y desde áreas que no necesariamente integran información conjunta.

Esto conlleva, a operar e informar de manera integrada, mostrando una organización balanceada en temas que sobrepasan el ámbito financiero pareciese ser el gran desafío como organización y para Auditoría Interna, generando la oportunidad de entregar una visión independiente para un aseguramiento razonable, que permita generar confianza y transparencia en un mercado que día tras día, lo requiere con mayor fuerza.

Para tener una aproximación holística a estas temáticas, los programas de trabajo que se definan para evaluar los factores ESG, debiesen estar alineados en un enfoque que considere el nivel de madurez actual de los tres pilares y las brechas existentes de acuerdo con las intenciones del Directorio, la Alta Administración y las regulaciones vigentes.

Centrándonos en los pilares como grandes ámbitos a considerar:

- Estrategia y Gobierno en temáticas financieras y no financieras.
- Desempeño de las organizaciones en materia ESG.
- Gestión de riesgos más allá de los temas financieros, ESG, Cyber, entre otros.

Bajo estos conceptos de acción, es fundamental para la Auditoría Interna, entender los grados de madurez existentes en cada uno de estos frentes de aplicación para decidir con cual de sus dos principales roles (Asesoría o Aseguramiento) es más efectivo apoyar al Directorio en movilizar a la organización.

Entrando en materia especifica de evaluación, existen algunas guías sobre aspectos mínimos a considerar en cada frente. Por ejemplo, en el Instituto de Auditores Internos a través de su publicación "AI y aspectos ESG" define los siguientes ámbitos de evaluación para cada Pilar:

Medioambiente
Environmental - E

Impactos medioambientales de la actividad, como la contaminación, el uso de recursos o la mitigación del cambio climático y la adaptación al mismo.

Los principales objetivos en ámbito ambiental (de acuerdo a la Taxonimía de la UE) son:

Cambio Climático:
- La mitigación del cambio climáticos.
- La adaptación al cambio climático.

Retos Ambientales:
- El uso sostenible y la protección de las aguas y demás recursos marinos.
- La transición a una economía circular.
- La prevención y control de la contaminación.
- La protección y restauración de la biodiversidad y los ecosistemas.

Social
Social - S

Impacto en la sociedad, la comunidad, la economía y los *stakeholders* en general.

Algunos de los principales objetivos en el ámbito social (de acuerdo al éstandar internacional de referencia Global Reporting Initiative; GRI) son:

- Erradicación de la desisgualdad social.
- Inclusión social.
- Mejora de las relaciones laborales.
- Inversión en capital humano.
- Protección de las comunidades locales e indígenas.
- Preservación del Patrimonio Cultural.

Gobierno
Governance - G

Inclusión de elementos de buen gobierno en las instituciones en reconocimiento del papel fundamental que tiene sobre los accionistas, clientes, colaboradores y todos aquellos a los que afectan sus decisiones empresariales.

Algunos de los principales objetivos en el ámbito de buen gobierno (de acuerdo al estándar internacional de referencia Global Reporting Initiative; GRI) son:

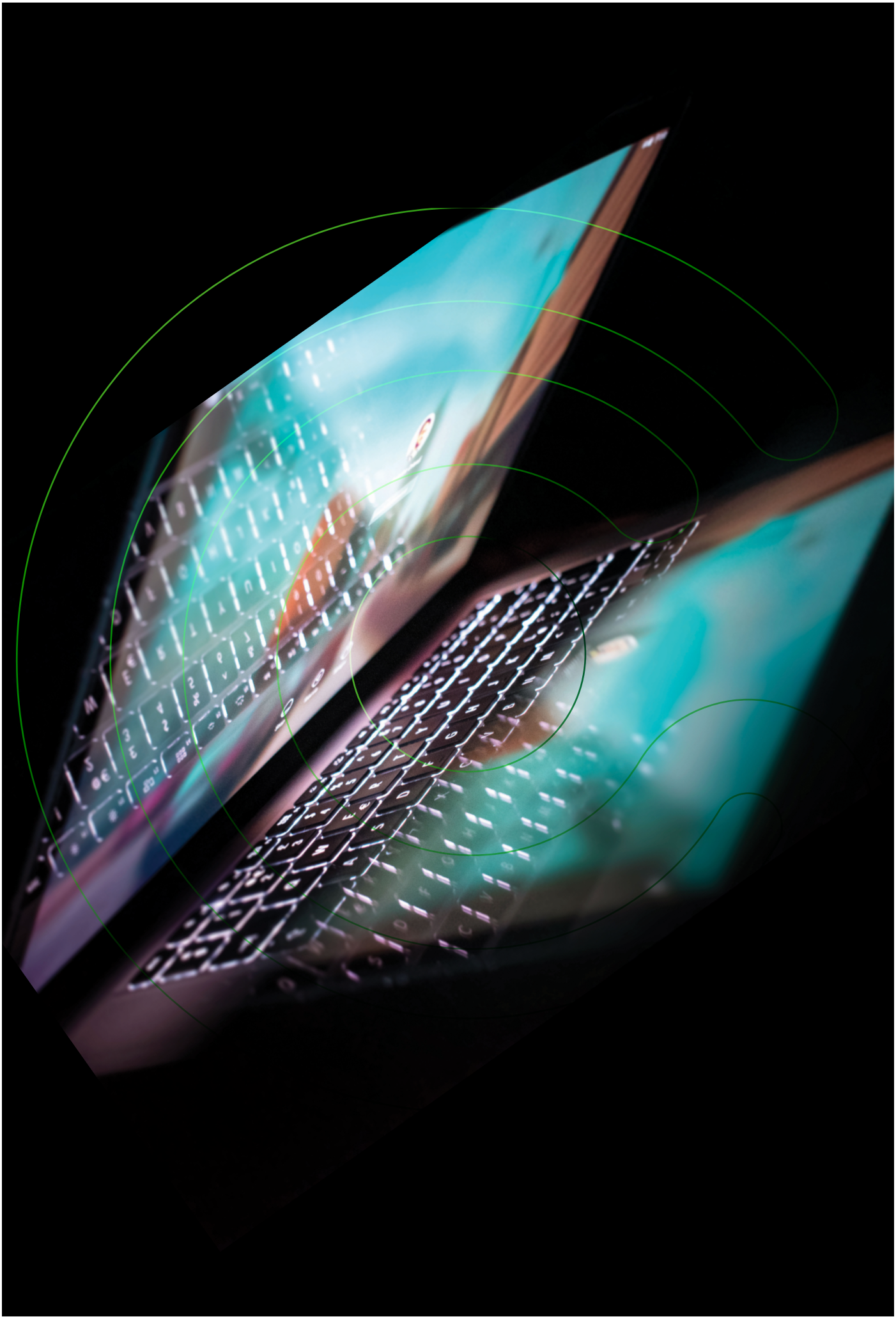
- Desarrollo de estructuras de gestión, liderazgo y relaciones internas sólidas.
- Fomento de la independencia en la toma de decisiones.
- Impulso a la transparencia y rendición de cuentas.
- Promoción de buenas prácticas.
- Lucha contra la corrupción y el fraude.

Esquema del marco de los principios ESG. Fuente: Management Solution (2020)

De acuerdo con estos parámetros, las principales conclusiones dan cuenta de un desafiante camino para la Auditoría Interna en cuanto a, cumplir con las expectativas del Comité de Auditoría y del Directorio, y de esta forma estar sintonizados con este cambio en la forma de reportar de la empresa, de relacionarse con la comunidad y sus ***stakeholders***.

Así mismo, esto genera oportunidades para continuar transitando hacia una transformación de Auditoría Interna en los ámbitos de manejo de información (datos) e indicadores, que para este proceso de gestión ESG, serán claves a la hora de evaluar el desempeño de las organizaciones en materia ESG. Deloitte, a su vez, en la evaluación de estos tres pilares, ha integrado las áreas de Auditoría Interna y ESG para revisar de forma estratégica estos factores, los cuales se suman a una larga lista de integraciones en esta materia, con el objetivo de dar aseguramiento a las compañías.

Esto tiene por objetivo llevar adelante procesos de control interno con verdaderas contrapartes (técnicas) al momento de evaluar procesos que requieren competencias específicas, como es el caso de los temas sociales y medioambientales.



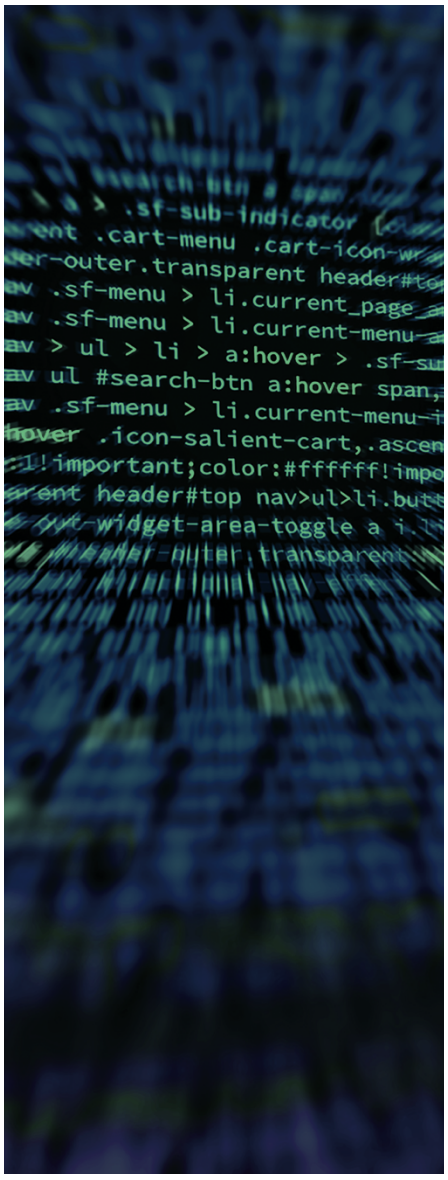
Compliance y la protección de los datos personales

Por **Juan Pablo González Gutiérrez** | Senior Manager, Data&Privacy.

La gestión de los riesgos de asociados al uso de la data personal nunca ha sido un tema fácil de abordar para las organizaciones, especialmente en países que cuentan con una baja cultura en la materia o derechamente, una normativa desactualizada.

Chile cuenta con una normativa en materia de protección de datos personales del año 1999 (Ley Nº 19.628, sobre Protección a la Vida Privada). Esta regulación se centra en propiciar el uso de la data personal por parte de las organizaciones, pero descuida aspectos centrales como el ejercicio efectivo de los derechos de los titulares, un conjunto de obligaciones claras para el responsable, la existencia de una Autoridad que pueda fiscalizar y sancionar su incumplimiento.

Las regulaciones modernas en la materia, particularmente el Reglamento General de Protección de Datos Personales (GDPR), promueve diversas formas de autorregularse basados en el principio de responsabilidad proactiva (accountability) que debe demostrar el responsable de las bases de datos que está utilizando dicha información acorde a los diversos aspectos que conforman la normativa. En ese mismo sentido, la existencia de Códigos de Conducta en ciertos mercados (artículo 40 y 41 GDPR), son un claro ejemplo, que a través de mecanismos de cumplimiento voluntario se pueden establecer reglas específicas para la correcta aplicación de la normativa, debiendo ser aprobados por la Autoridad de Protección de Datos Personales nacional, y pudiendo, inclusive tener aplicación local o transfronteriza[1].



El fenómeno de la autorregulación se ve reflejado en el Proyecto de Ley sobre Protección de Datos Personales que crea una

[1] Disponible en: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/codigos-de-conducta

Agencia en la materia (Boletín Nº 11.144-07)[2], en sus artículos 49 y siguientes del texto aprobado en el Senado (primer trámite constitucional) permitiendo que voluntariamente las organizaciones adopten un modelo de prevención de infracciones, que establezca un programa que gestione los diversos riesgos asociados a los usos de los datos personales de la organización. A modo general, este programa debe ser promovido por la Alta Dirección a través de la designación de un encargado de prevención o delegado de protección de datos personales, que cuente con los medios y facultades para implementarlo dentro de la organización. Este programa debe: identificar el tipo de información que trata la organización y los tipos de datos personales; las actividades o procesos de la entidad, habituales o esporádicos, que pueden cometer la infracción a la regulación; la existencia de protocolos, reglas y procedimientos en materia de protección de datos personales; mecanismos de reporte interno como a las autoridades; sanciones administrativas, entre otros. Este Modelo de Prevención puede ser certificado por la Autoridad de Protección de Datos Personales y otorga una atenuante a la organización en caso de infracción de la normativa.

Entonces, ¿de qué sirve la autorregulación, si, finalmente puedo incurrir en incumplimiento de la normativa de todas formas? Bueno, contar con un programa que haya identificado claramente las actividades de riesgo de infracción de la normativa en materia de protección de datos personales y haber aplicado acciones concretas al respecto, permite que cualquier responsable como encargado (ej. Aquél tercero a quien le pido que procese información por cuenta de quien se lo encarga) pueda acreditar ante una autoridad fiscalizadora que se adoptaron medidas organizativas y técnicas para generar no solo contar con políticas o cláusulas contractuales, sino también crear una cultura de respeto a los derechos de las personas que usan su información. Este elemento ha sido altamente valorado por las autoridades internacionales, puesto que permite acreditar que el asunto es de relevancia dentro de la organización y se están realizando actos positivos para avanzar desde un cumplimiento formal hacía uno material, en favor de entender que usar datos de personales implica un riesgo, pero la normativo no lo prohíbe en todos los casos, sino que insta a que las organizaciones sean responsables de gestionarlo adecuadamente.

[2] Actualmente se encuentra en Segundo Trámite Constitucional en la Cámara de Diputados, en la Comisión de Constitución, Legislación, Justicia y Reglamento. https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=11661&prmBoletin=11144-07

Desafíos del Compliance ante la modificación de la Ley Nº 21.459 sobre Delitos Informáticos

Por **Oscar Martínez Yvirmas** | Gerente Risk Advisory

El fenómeno de la ciberdelincuencia en las compañías se ha tornado un dolor de cabeza para las áreas de ciberseguridad, puesto que en el último período han incrementado enormemente los ataques informáticos, como, por ejemplo: ransomware (secuestro de datos) o accesos no autorizados y su filtración a terceros, por ejemplo, los sufridos en sectores regulados en nivel Latinoamérica.

Ello, no solo ha generado un impacto importante para estas áreas y han tenido que fortalecerse para dar respuesta a estos desafíos, ya que dichos ataques informáticos varias veces pueden implicar un alto riesgo de infracciones de algunas regulaciones y, por ende, la obligación de reporte a Superintendencias o autoridades judiciales, por ejemplo. En este punto, las áreas de cumplimiento se vuelven actores relevantes para afrontar correctamente estas situaciones de contingencia.

Ahora bien, si relacionamos esta situación a los requerimientos de la normativa "Ley Nº 21.459 sobre Delitos Informáticos", que incorpora de manera expresa a los ilícitos informáticos en los sistemas de cumplimiento de las compañías, el escenario se tornar un poco más complejo.

Recordemos, que la Ley Nº 20.393 sobre Responsabilidad Penal de las Personas Jurídicas atribuye la responsabilidad penal en cuanto al defecto organizacional, es decir, que debido al incumplimiento de los deberes de dirección y supervisión que tienen los sujetos señalados en el art. 3º de la citada norma, que son relacionada con Alta Dirección o Gerencia de una compañía.

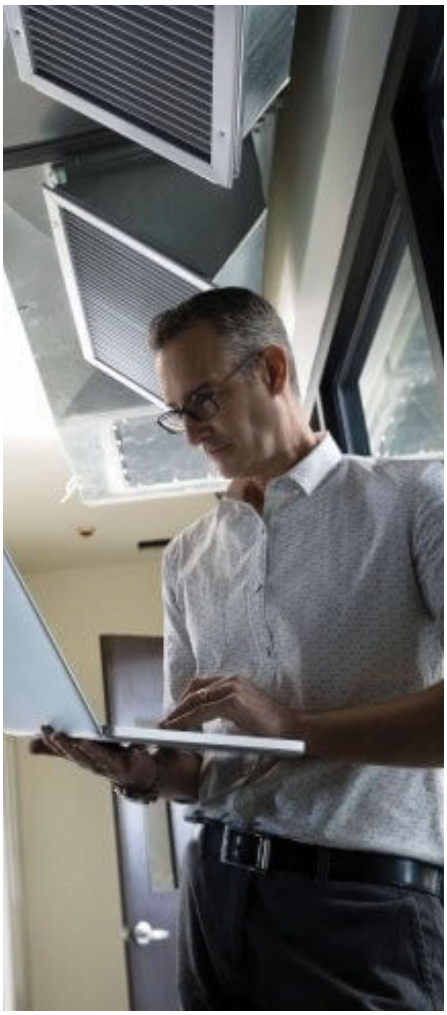
Hay que tener presente, que la eximente de responsabilidad penal (o atenuante, si procediese) se configura en cuanto exista un sistema que permite identificar las actividades, ya sea habituales o esporádicas, que permita la realización o incremento el riesgo de los delitos, entre ellos ahora los informáticos. Es importante mencionar, que la comisión del ilícito debe reportar un interés o provecho para la persona jurídica, expresiones que ha generado complejidades al momento de identificar especialmente en materia informática en cuanto a cómo se configura este "interés o provecho"; No obstante, a nivel internacional los ejemplos se presentan desde actividades en ciertos mercados competitivos hasta derechamente, ingresar a un sistema de un tercero e inutilizarlo.

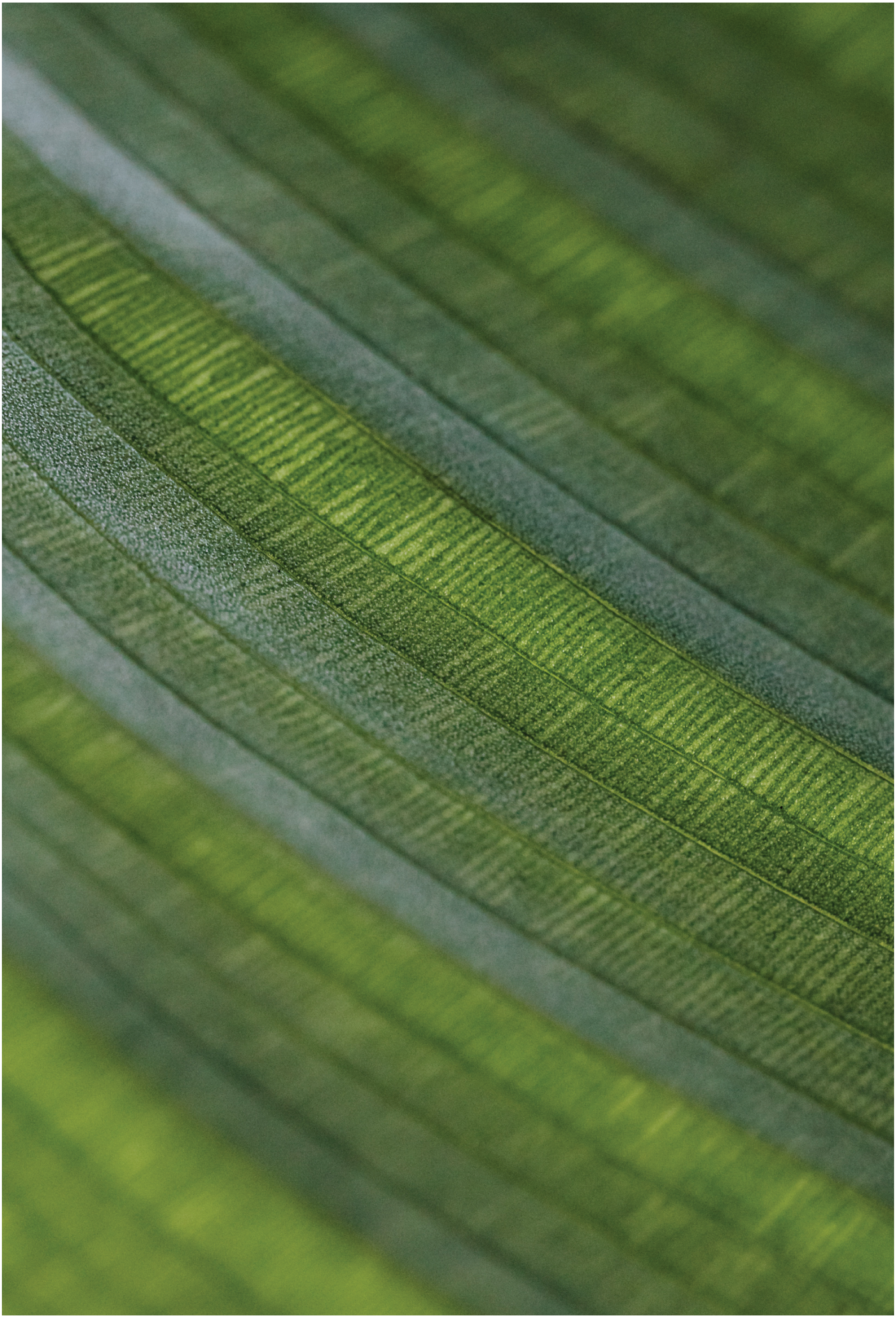
Ante este desafío emergente, las organizaciones deben ser capaces de diseñar y adoptar un programa de cumplimiento enfocado a las necesidades del entorno y al perfil de riesgos organizacionales para

prevenir la ciberdelincuencia, entre los elementos claves a considerar en el programa se encuentran:

- **Identificación:** Identificar los riesgos en materia de ciberdelincuencia a los que se enfrenta la organización, teniendo en consideración el impacto y la probabilidad de que se materialicen.
- **Prevención:** Una vez identificados los riesgos, se deben diseñar, implementar y evaluar procedimientos (controles) que protejan a la organización y mitiguen los riesgos identificados.
- **Monitoreo continuo:** La eficacia de los controles implementados debe ser monitoreada de forma continua, a objeto de garantizar que los mismos se encuentren operando.
- **Generación de cultura:** Paralelamente, la Alta Administración y todos los stakeholders de la organización, deben ser capacitados, entregándoles información necesaria para llevar a cabo sus labores de acuerdo con los cambios normativos y con el objetivo de impedir debilidades internas.

Finalmente, la función de Cumplimiento debe poner un foco de atención cada vez más importante en los diversos aspectos asociados a la transformación digital en las compañías, con el objetivo de reducir las potenciales debilidades internas y potenciar las capacidades internas asociadas a la incorporación de diversas tecnologías para operar con un grado de "ciberseguridad razonable", en entornos cada día más conectados con la tecnología.





Modernización de la función de Ética y Cumplimiento “De protección del valor a creación del valor”

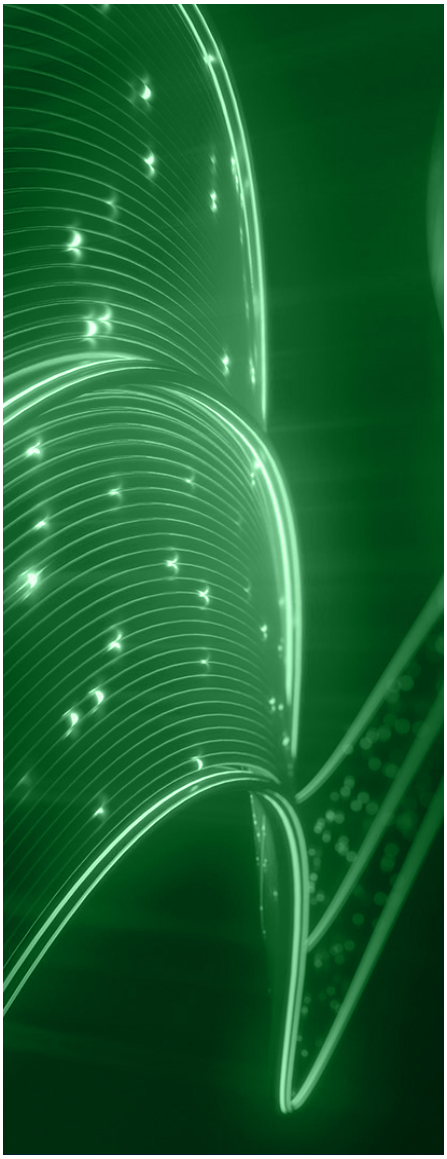
Por **Oscar Martínez Yvirmas** | Gerente Risk Advisory

El cimiento de la función de Compliance consiste en prevenir, detectar, responder y remediar los riesgos de cumplimiento que viven cada día las organizaciones.

Ejecutar las actividades diarias de Compliance es una labor primordial para los Oficiales de Cumplimiento y sus equipos, sin embargo, estas actividades absorben casi la totalidad del tiempo que podría ser utilizado para mitigar los riesgos de Cumplimiento de forma prospectiva. Una función tradicional de Compliance puede esperar recibir crédito sólo por mantenerse a flote. Sin embargo, ¿Cómo puede llegar a la siguiente etapa y comenzar a agregar valor?

El primer paso consiste en reconocer que la función de Compliance en una organización progresa a través de diferentes niveles de madurez: Por un lado, existe un estado fundamental que se logra trabajando bajo enfoques tradicionales “inventarios de regulatorios, evaluación de riesgos, políticas de cumplimiento y programas de capacitación, otros” y por otro, se alcanza un estado modernizado cuando existe un modelo de gobierno con directrices claras, herramientas de vanguardia, tecnología analítica; el número y naturaleza de sus conexiones con otros departamentos del negocio; las expectativas asignadas a la función y mucho más.

Las funciones de Compliance más avanzadas llegan a un estado de madurez absoluto cuando agregan valor a cada una de las unidades de negocio con quien interactúa, por lo que es importante que cada organización realice un diagnóstico y decida cuidadosamente en qué nivel quiere estar en ese espectro de madurez y posteriormente, desarrollar una hoja de ruta, para desplegar iniciativas concisas y hacer que ocurran.



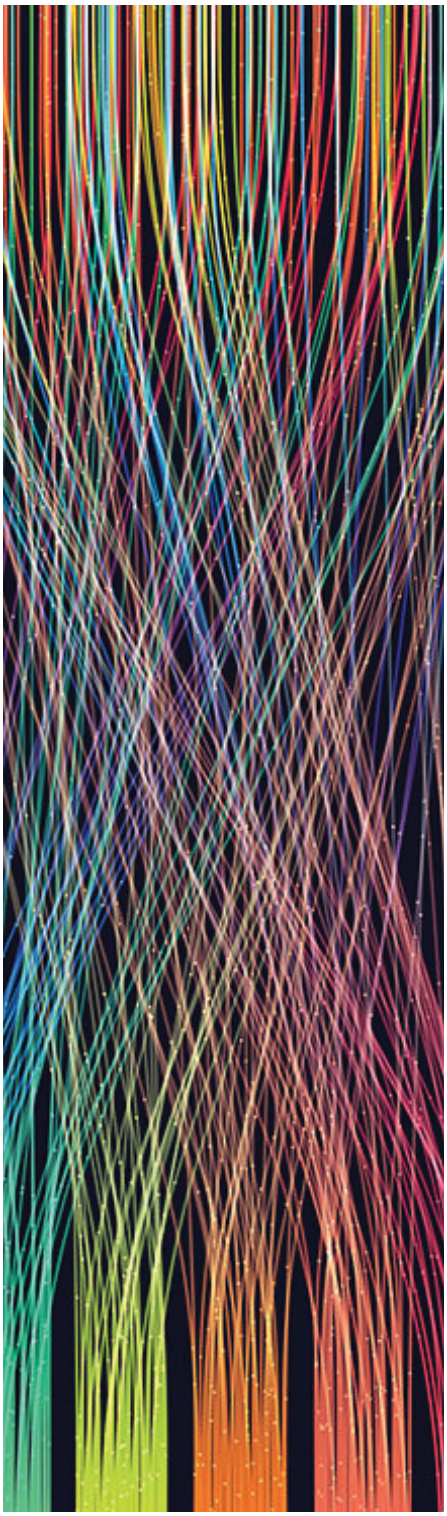
Un sistema de Compliance modernizado toma las actividades tradicionales y las mejora continuamente, considerando qué:

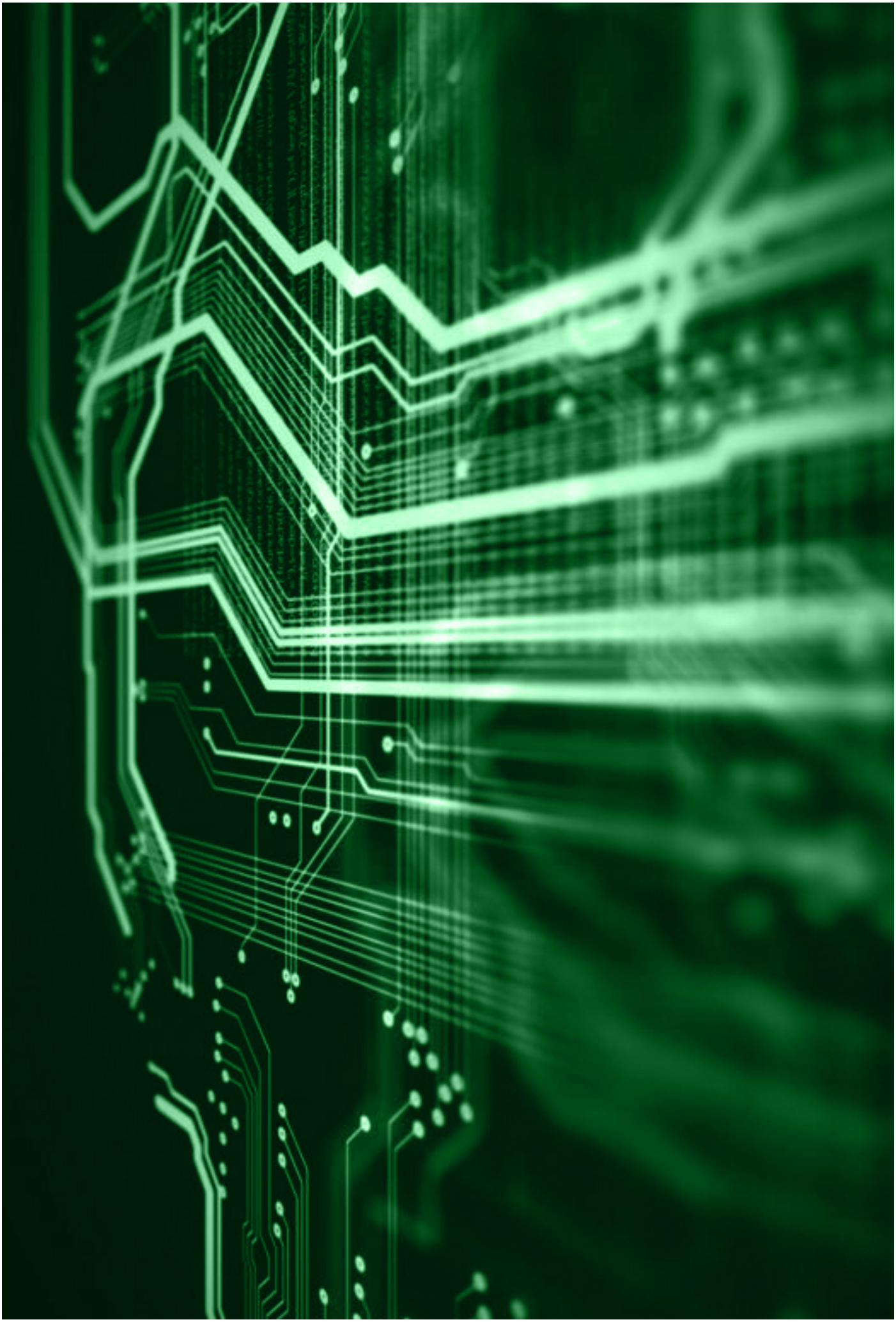
- Incorpora una cultura ética e incentivos apropiados al Cumplimiento y viceversa, en este punto se impulsa el comportamiento deseado de cada uno de los stakeholders con los que se relaciona la organización.
- En lugar de simplemente identificar roles, un sistema de Compliance modernizado busca una base de talento más enfocada en perspectivas y orientada a riesgos por procesos y cultiva a la gente dentro de la organización que encaja en la nueva normalidad.
- Los procesos de monitoreo y testeo comienzan a racionalizarse para impulsar mejor cobertura y confianza en las tres líneas de defensa y otras disciplinas de riesgos ("operacionales, ciberseguridad, reputacionales, otros").
- A las tres áreas de capacidades del modelo operativo clásico "gente, proceso y tecnología," el Compliance modernizado agrega una cuarta: análisis proactivo de datos.

¿Por qué las organizaciones deben invertir en un nivel más avanzado de administración de riesgos de Cumplimiento?

Cada organización tiene un desafío implícito: ¿Qué tanto cumple tu organización? Por lo que es indispensable:

- **Profundizar el rol de la función de Compliance** en la planeación estratégica de la Organización y con ello, impulsar su incorporación en las decisiones claves.
- **Mayor necesidad de coordinación,** en lugar de los silos del pasado, las organizaciones modernas necesitan estrategias y modelos de confianza alimentados por datos que mantengan a sus funciones de administración de riesgos en la misma página.
- **Impulsar una visión holística de riesgo y cumplimiento,** desde predecir hasta actuar y monitorear.
- **Mayor responsabilidad individual,** las organizaciones están sujetas a fiscalizaciones más rigurosas y multas más elevadas con la particularidad de que los colaboradores, también enfrentan responsabilidad individual.





Trazabilidad de la prueba electrónica

Por **Pedro Trevisan** | Socio FA, Deloitte.

En el mundo digital en el que vivimos y debido al creciente uso de todo tipo de dispositivos electrónicos, las fuentes de pruebas de carácter digital han aumentado exponencialmente.

Así, la nueva Ley de Delitos Informáticos próxima a publicarse, introduce una nueva norma sobre el tratamiento de los datos para efectos de ser considerados como prueba en juicio, agregando al Código Procesal Penal la facultad de Ministerio Público para requerir de los proveedores de servicios de telecomunicaciones, la retención o captura de la información digital asociada a un caso hasta por noventa días.

Esta nueva norma, se suma otras anteriores que han establecido los requisitos de integridad y completitud de la prueba electrónica. Requiriéndose siempre para su tratamiento, de medidas técnicas específicas, que permitan garantizar que la data no ha sido alterada o manipulada desde su adquisición, hasta el momento en que será usada potencialmente en un juicio.

En cualquier jurisdicción, las pruebas electrónicas que se aporten en los procedimientos judiciales deben presentarse de forma que se garantice un trabajo objetivo, repetible y rastreable. Así, aunque uno de los principales retos de los procesos de eDiscovery es la gestión de enormes volúmenes de información relacionada con un caso, es absolutamente necesario tener en cuenta en todas las fases del proceso que los resultados pueden acabar incorporándose a un procedimiento judicial.

Por ello, desde la fase de acceso y obtención de la información en formato electrónico, es necesario que ésta sea adquirida y examinada según las mejores prácticas en informática forense, garantizando en todo momento la cadena de custodia.

Además, dado el uso cada vez más intensivo de la tecnología en todos los ámbitos de la empresa, el objetivo va a veces más allá de la clasificación o la gestión de grandes volúmenes de información, lo que lleva a una labor más detallada de peritaje técnico-informático, que explica el funcionamiento de los sistemas y su operación.

Ante este nuevo reto, surgen preguntas que requieren respuestas, como las siguientes:

- ¿Qué ocurrió en algún momento en los sistemas de la empresa?
- ¿Quién podría estar detrás de tal o cual acción o irregularidad?
- ¿Cómo se produjo un determinado proceso?
- ¿Qué medios y/o dispositivos electrónicos podrían haberse utilizado?
- ¿Podrían haber extraído información de la empresa que podría ser contraria a sus intereses?
- ¿Quiénes participaron dentro y/o fuera de la empresa?

La utilidad de estos procesos, que nos permiten obtener prueba o evidencia de que determinada acción o hecho ha sido cometido, reside en que los Tribunales puedan contar con información integra, trazable y una opinión técnica independiente.

En aquellos casos en los que la controversia tiene relación directa con la operativa de un determinado sistema informático (posible manipulación de datos, asuntos de propiedad intelectual o industrial, incumplimientos contractuales sobre la operativa de un determinado sistema, etc.), resulta imprescindible la validación técnica forense de un experto.

Más aún, en casi cualquier otra disputa, sería recomendable que la información en formato electrónico que se aporte cuente con una garantía de integridad y no manipulación, siendo los procedimientos forenses de adquisición, resguardo y cadena de custodia, un estándar que debiese alcanzarse frente a toda prueba electrónica.

Rosario Norte 407
Las Condes, Santiago
Chile
Phone: (56) 227 297 000
Fax: (56) 223 749 177
deloittechile@deloitte.com

Av. Grecia 860
3rd floor
Antofagasta
Chile
Phone: (56) 552 449 660
Fax: (56) 552 449 662
antofagasta@deloitte.com

Alvares 646
Office 906
Viña del Mar
Chile
Phone: (56) 322 882 026
Fax: (56) 322 975 625
vregionchile@deloitte.com

Chacabuco 485
7th floor
Concepción
Chile
Phone: (56) 412 914 055
Fax: (56) 412 914 066
concepcionchile@deloitte.com

Quillota 175
Office 1107
Puerto Montt
Chile
Phone: (56) 652 268 600
Fax: (56) 652 288 600
puertomontt@deloitte.com

Deloitte.

www.deloitte.com

Las partes aceptan que COVID 19 constuye Fuerza Mayor, conforme los términos del artículo 45 del Codigo Civil. Asimismo, Las partes reconocen los riesgos que implica la propagación de la COVID-19 y las repercusiones potenciales asociadas con la prestación de los Servicios. El personal de las partes cumplirá con las restricciones o las condiciones que impongan sus res pectivas organizaciones en las prácticas laborales a medida que la amenaza de la COVID-19 continúe. Las partes intentarán seguir cumpliendo con sus obligaciones respectivas conforme a los plazos y el método establecido en la presente, pero aceptan que puede requerirse la adopción de prácticas laborales alternativas y la puesta en marcha de salvaguardas durante este periodo, tales como el trabajo a distancia, las restricciones de viaje relacionadas con destinos particulares y la cuarentena de algunas personas. Dichas prácticas y salvaguardas laborales pueden afectar o impedir la ejecución de diversas actividades, por ejemplo, talleres u otras reuniones en persona. Las partes trabajarán conjuntamente y de buena fe a fin acordar los eventuales cambios necesarios para atenuar los efectos negativos de la COVID-19 sobre los servicios, incluido el cronograma, el enfoque, los métodos y las prácticas laborales en la prestación de los mismos, y todos los costos asociados adicionales. En todo caso, Deloitte no será responsable de cualquier incumplimiento o retraso en la ejecución de sus obligaciones ocasionados o exacerbados por la propagación de la COVID-19 y sus efectos asociados.