Protección & Seguridad
Enero - Febrero / 2023

Transformación digital: retos en la gestión de la información corporativa y otros desafíos





Daniel Peña Valenzuela
Abogado de la Universidad Externado de Colombia
Magíster en Propiedad Intelectual y Nuevas Tecnologías / Estudios de profundización en Derecho Internacional en La Haya y en Arbitraje Internacional en la Cámara de Comercio Internacional / Profesor Ordinario de la Universidad Externado de Colombia / Árbitro y panelista de nombres de dominio de internet del Centro de Arbitraje y Mediación de la Organización Mundial de la Propiedad Intelectual OMPI y Cámaras de Comercio de Bogotá y Medellín / Socio fundador de la firma Peña Mancero Abogados.

La transformación digital trae consigo oportunidades y retos para las empresas. A la par, los riesgos legales se incrementan como consecuencia del necesario cumplimiento normativo previsto para las actividades del ecosistema digital, así como por las regulaciones de ciertos negocios digitales. Nuevos cargos y funciones aparecen al interior de las empresas con estándares de responsabilidad y deberes respecto al *compliance* [1].

[1] Expresión de origen anglosajón que agrupa las áreas de cumplimiento normativo usual en las empresas sometidas en alguna medida de supervisión, vigilancia y control por parte del Estado.

Introducción

La transformación digital comprende el uso aplicado, avanzado y práctico de Tecnologías de la Información y las Comunicaciones (TIC) por parte de las empresas, así como por los gobiernos y los ciudadanos. En las empresas esta transformación en curso está asociada tanto a la necesidad de mejorar la productividad y competitividad como al propósito de agilizar procedimientos internos, disminuir costos y mejorar los canales de comunicación con clientes. En ese sentido, el impacto de la transformación digital en el aparato productivo, así como en los canales de comercialización de productos y servicios redundaría en un mercado más eficiente y en mayor bienestar para los consumidores.

En este artículo se analiza el impacto legal del uso empresarial de las tecnologías emergentes. Para considerar los riesgos asociados a la transformación digital empresarial se toma como base el hecho de que los administradores tienen deberes generales, así como un rol fundamental de liderazgo en el diseño, planeación y cumplimiento legal asociado a las estrategias enfocadas en TIC.

A su vez, se analiza el papel de nuevos cargos que surgen en este contexto como los vicepresidentes de Información y Tecnología (CIO), los *web master* y los *community manager* teniendo en cuenta que, además de los deberes propios de sus roles, las actividades que desempeñan pueden originar responsabilidad legal frente a la empresa, los terceros, los reguladores y las autoridades.

> *"En las empresas esta transformación en curso está asociada tanto a la necesidad de mejorar la productividad y competitividad como al propósito de agilizar procedimientos internos, disminuir costos y mejorar los canales de comunicación con clientes".*



La aparición de tecnologías emergentes para uso empresarial

Hasta hace poco las tecnologías que se utilizaban al interior de las empresas estaban confinadas a un número reducido de posibilidades como el mero licenciamiento de programas de computación y, en algunos casos, el uso incipiente de bases de datos con información sobre empleados, clientes y proveedores. Sin embargo, hoy por hoy, el inventario de TIC en el ámbito empresarial no solo ha evolucionado sino que se ha incrementado de una manera significativa para incluir tecnologías emergentes como, por ejemplo, páginas web corporativas, dominios de internet, plataformas de comercio electrónico, desmaterialización documental (comunicaciones, documentos y facturación electrónica), perfiles corporativos en redes sociales, aplicaciones móviles, *big data,* mercadeo y publicidad digital, posicionamiento orgánico (SEO), virtualización de procesos y computación en la nube. Incluso, varias empresas e industrias están dando un paso más allá y han empezado a incorporar en sus procesos y actividades la realidad virtual y aumentada, la robótica, la impresión 3D, el uso de drones y la inteligencia artificial.

Todas estas nuevas TIC se utilizan cada vez con mayor frecuencia en las empresas tradicionales, las cuales exploran, investigan, prueban e incorporan sus ventajas y bondades a los procesos productivos, de mercadeo y de logística. A su vez, son empleadas para desarrollar modelos de negocio específicos de empresas digitales.

No obstante, muchas de estas TIC no tienen regulación en cuanto a su explotación y uso comercial con lo cual se generan inquietudes y obstáculos prácticos, así como costos de transacción para su utilización debido a la incertidumbre sobre las bases y límites frente a la responsabilidad legal que puede traer consigo su utilización (Ceruzzi, 2003).

La transformación digital surge como consecuencia, entre otras, de la masificación comercial del software y, más

recientemente, de la disrupción causada por la analítica de datos, el internet de las cosas, la robótica y la inteligencia artificial, elementos que estarían introduciendo una nueva revolución industrial en la cual la producción a la medida, la aparición de nuevos materiales y la masificación de las impresoras 3D puede cambiar los factores y variables tradicionales de la producción industrial (Anderson, 2012).

Nuevos roles y cargos relacionados con las TIC al interior de las empresas

La transformación digital es individual y empresarial. La cultura digital propicia la aparición de usuarios generadores de contenido y, al mismo tiempo, cada persona acumula la condición de consumidor digital, usuario de servicios TIC y ciudadano digital. Esas tres dimensiones individuales difieren en países desarrollados y emergentes debido a las condiciones de acceso a la red y de alfabetización digital de la población.

La otra faceta de la revolución TIC es la empresarial, fruto de la relevancia de los sistemas de información al interior de las empresas, así como de la especialización y sofisticación de las funciones que estos cumplen, lo cual ha obligado a las empresas a reorientar su visión con respecto a la gestión, manejo y administración interna de las TIC y de la información misma.

Las empresas usualmente tienen dos opciones. Una se enfoca en ampliar sus departamentos internos de TIC vinculando a expertos en internet, redes sociales y soluciones informáticas, así como en capacitar o profesionalizar en las tecnologías emergentes al recurso humano que está bajo el control del área de tecnología. La otra alternativa es contratar la tercerización de servicios informáticos con proveedores mediante contratos de *outsourcing* y acuerdos de niveles de servicios (SLAs). Ambos modelos dan lugar a responsabilidad ya que el hecho de que una empresa encargue a terceros el procesamiento de la información o la propiedad de los equipos no da lugar a la transferencia de la responsabilidad. De hecho, es relevante la manera en la que los contratos de *outsourcing* se establecen cláusulas de confidencialidad, niveles de seguridad y servicios, entre otras responsabilidades en caso de la materialización de eventos que afecten la integridad y seguridad de la información.



En el caso de los datos personales, la Ley 1581 de 2012 establece de manera expresa los deberes de los responsables y encargados del tratamiento de la información personal con el fin de que se no diluyan las cargas y obligaciones de cada uno de ellos. De igual manera, en el caso de los productos o servicios digitales, tampoco se debe dejar de lado la responsabilidad entre productor y distribuidor frente al consumidor. En otras palabras, la novedad del formato no afecta la regla general de solidaridad.

Ahora bien, uno de los desarrollos más interesantes y, a la vez, más preocupantes en el entorno empresarial es el hecho de que la transformación digital propicia que los usuarios de tecnologías sean, al mismo tiempo, generadores de contenidos. Esta vocación creadora de los empleados coincide con la incorporación en el mundo laboral de la denominada "generación del milenio", es decir, jóvenes nativos digitales de la era tecnológica que comienzan a ingresar a las empresas como nueva fuerza de trabajo.

Esta tendencia de usuarios creativos agrega nuevos desafíos jurídicos ya que los empleados — ahora generadores de contenidos en redes sociales — presentan opiniones, revelan información propia y de la compañía e interactúan con otros empleados a través de las plataformas digitales, lo que puede generar responsabilidad para la empresa por infracción a los derechos de terceros o de la propia empresa y afectar la reputación corporativa a escala global y en tiempo real (Rallo & Martínez, 2013).

Además de los ingenieros que, tradicionalmente, controlaban el funcionamiento cotidiano de los sistemas de información, diversos profesiones y oficios irrumpen en el ámbito empresarial con múltiples capacidades como el diseño de contenidos digitales, la programación de aplicaciones, el mercadeo y la publicidad digital, la comunicación de mensajes en el ecosistema digital, el análisis de grandes volúmenes de datos, el periodismo por medios electrónicos, los blogueros e incluso, la psicología del consumidor en línea.

Desde el punto de vista jerárquico, el principal rol en la cúspide de la estrategia de la información en una empresa lo cumple el Chief Information Officer (CIO)[2] que es el encargado a nivel directivo de la planificación de la estrategia con respecto a la gestión y el valor agregado que debe generar la información para una organización. La gestión, tratamiento y administración de la información incluye, de manera preponderante, la determinación y valoración de los riesgos y las políticas de mitigación de estos así como las directrices en seguridad informática. Entre las principales habilidades que debe tener un CIO se encuentran: capacidad para orientar la relación de la tecnología con los negocios; destreza para determinar y encaminar los beneficios de la tecnología de la información hacia los problemas y retos del modelo de negocio de la empresa; pericia para identificar y evaluar las nuevas tecnologías que sean beneficiosas para el negocio; formación en seguridad informática y administración de costos y riesgos; facilidad para comunicarse y entenderse con clientes internos que no sean técnicos y habilidad para traducir al lenguaje gerencial la terminología técnica.

En este sentido, la visión estratégica se construye a partir de una clasificación o segmentación de la información que permita determinar su valor comercial y para el modelo de negocio específico, el ciclo de vida de la información entre su recolección y tratamiento final, la explotación de los resultados y su guarda o almacenamiento por el tiempo que sea adecuado. Desde el punto de vista legal, esta clasificación del valor de la información debe tener como base la definición de si se trata de información confidencial, pública, comercial, personal (datos personales públicos, semiprivados, privados o sensibles) así como del régimen legal que la cobija, el cual define los deberes legales y tecnológicos en cuanto a su reserva, acceso, tratamiento, actualización y transferencia a terceros (dentro y fuera del territorio nacional).



La gestión, tratamiento y administración de la información incluye, de manera preponderante, la determinación y valoración de los riesgos y las políticas de mitigación de estos así como las directrices en seguridad informática".

Otro nuevo rol en las empresas es el *web master* que es la persona responsable del mantenimiento y programación de un sitio web, de la disponibilidad de la información y, si es el caso, de las transacciones electrónicas. El *web master* tiene a su cargo clasificar y determinar, de acuerdo con las políticas de la empresa, la información que se va a publicar en la página y debe tener certeza de la titularidad de derechos de la organización sobre los contenidos digitales para evitar reclamos posteriores de empleados o de terceros. También debe tener a su cuidado la actualización de la información para que no se afecte la integridad o actualidad de los datos.

Del mismo modo, aparece el *community manager*[3] que es la persona encargada de construir, gestionar y moderar a los usuarios de las redes sociales y las comunidades virtuales en torno a una empresa u organización. Este cargo tiene un perfil delimitado al interior de aquellas empresas que pretenden obtener reconocimiento y reputación con base en las conversaciones sociales y la comunicación con los consumidores, usuarios y seguidores en línea. A nivel micro, es el encargado de generar los contenidos de las redes sociales y de lograr que la estrategia digital esté alineada a la imagen corporativa y los

[2] También denominado CTO Chief Technology Officer con alcance más amplio.

[3] La integración de medios digitales, redes sociales y aplicaciones móviles ha modificado y ampliado el rol del Community Manager para nominarlo como Digital Strategist o Estratega digital

valores empresariales, lo que asegura la coherencia de los contenidos móviles en las distintas plataformas y evita que la información pueda afectar la imagen, buen nombre o reputación de terceros. Este rol tiene, además, la función de observar a la competencia y generar publicidad a favor de las marcas propias, pero sin incurrir en prácticas desleales o infracciones marcarias.

Las funciones específicas de cada uno de estos cargos deben estar definidas en los documentos de estrategia y política que defina el CIO y en el organigrama de la empresa para establecer sus actividades, deberes y limitaciones y, con base en lo anterior, el grado de responsabilidad como garantes de la integridad y autenticidad de la información empresarial.

Los modelos de negocio como estándar de la responsabilidad de la empresa

En Colombia, la Ley 1341 de 2009 establece la intervención del Estado en el sector TIC y configura los deberes y obligaciones de las empresas que son proveedoras de servicios y redes TIC como servicios públicos a cargo del Estado, pero que pueden ser prestados por particulares.

> *Las obligaciones legales que deben cumplir las empresas en relación con la tecnología incluyen la protección de datos personales, las normas de competencia de los mercados digitales y los derechos de autor en la era digital, entre otros."*

Las obligaciones legales que deben cumplir las empresas en relación con la tecnología incluyen la protección de datos personales, las normas de competencia de los mercados digitales, los derechos de autor en la era digital, la protección del nombre y enseña comercial de los establecimientos de comercio virtuales, así como la protección jurídica de los nombres de dominio de internet. Estas normas tradicionales permiten la determinación del régimen de propiedad y explotación de bienes inmateriales.

Por ende, existen leyes y reglamentos aplicables al entorno digital y a la equivalencia de funciones y efectos jurídicos como la ley 527 de 1999 que se aplica a la prueba digital, a las actividades de comercio electrónico, las entidades de certificación digital, entre otras.

Estas normas han sido introducidas en el ordenamiento jurídico colombiano (y en casi todos los países del mundo) con el fin de responder a la primera etapa de utilización de medios electrónicos para actividades con relevancia mercantil. Por ejemplo, en relación con la responsabilidad, se pueden resaltar los deberes y obligaciones de los suscriptores de certificados digitales en cuanto a la diligencia y cuidado con respecto a las claves privadas, así como la información que deben entregar a las entidades de certificación sobre cualquier cambio. Así mismo, incluyen los deberes y responsabilidades en cuanto a Políticas de Certificación para entidades certificadoras y el debido cumplimiento de los requisitos de acreditación.



También se establecen regulaciones específicas de internet para los proveedores de este servicio como las relacionadas con los derechos de los usuarios en los contratos de acceso, los estándares de las tecnologías de banda ancha, deberes en cuanto a la no discriminación de contenidos y neutralidad en la red, la lucha universal contra la pornografía infantil, la defensa contra la piratería o infracción de derechos de propiedad intelectual (Peña, 2013) o la retención de información de los usuarios sobre el tráfico en la red.

Finalmente, existen regulaciones sectoriales de actividades específicas cuando se llevan a cabo utilizando canales digitales (banca electrónica, televisión digital o por protocolo de internet), juegos de azar, actividades profesionales y venta de medicamentos, en lo que se

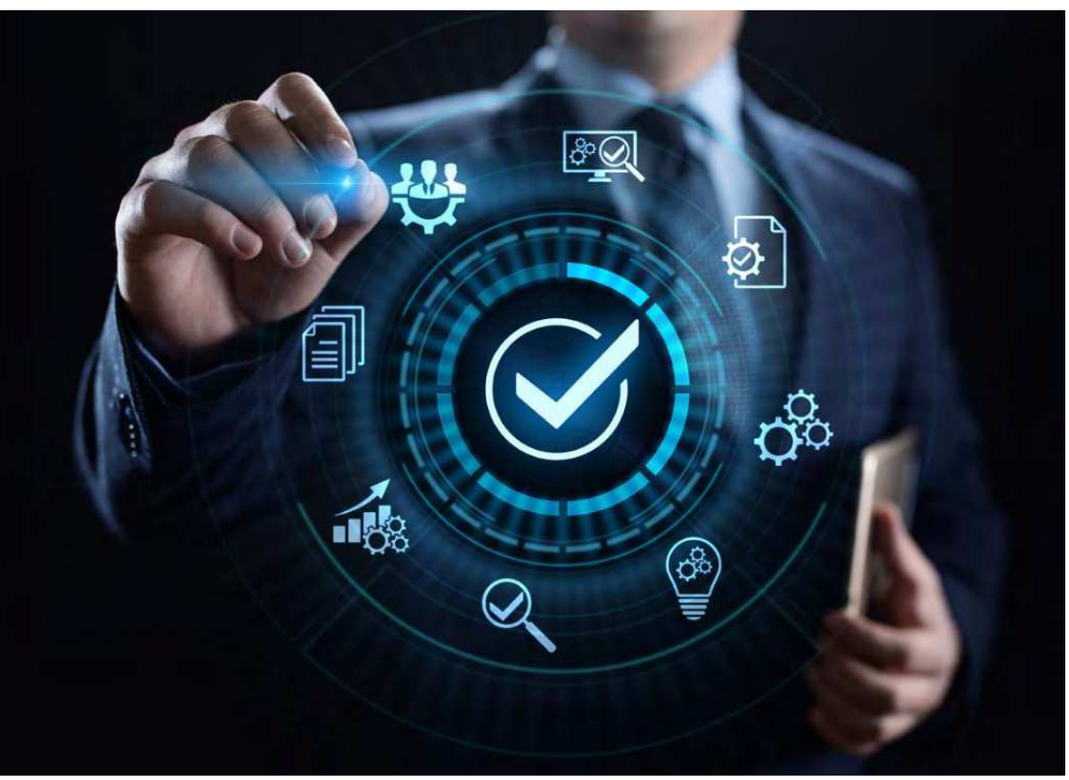
refiere a estándares de seguridad informática o límites en la prestación de ciertos servicios.

Riesgos asociados a la digitalización

La estrategia o agenda digital bajo la planificación del CIO y con la responsabilidad de ejecución por parte del *web master*, el *community manager* o el estratega digital debe ser parte del plan de acción de aquellas empresas, de cualquier tamaño, que pretendan competir en el mercado de manera adecuada; implementar la gestión de la innovación, la ciencia y la tecnología; ingresar en nuevos mercados aprovechando la eliminación o disminución de las barreras; entrar en un proceso de internacionalización y/o insertarse en la economía digital y en la sociedad de la información para aprovechar las dinámicas de la globalización.

Pese a estas oportunidades, las organizaciones deben tener en cuenta los riesgos que conlleva la digitalización de sus actividades y la desmaterialización de documentos y procesos. Algunos de estos son:

1. La pérdida de acceso a la información corporativa y a su disponibilidad.
2. La repudiación de las comunicaciones electrónicas y mensajes de datos enviadas por la empresa a terceros.
3. La aplicación por analogía de normas o regulaciones tradicionales a las actividades por medios electrónicos.
4. La afectación a derechos fundamentales de terceros como el derecho a la intimidad, a la protección de datos personales, a la libre expresión y al libre desarrollo de la personalidad.
5. El ejercicio de nuevos derechos por parte de los consumidores en línea como el derecho de información reforzada, el derecho de retracto y la reversión de pagos en los cuales cuentan con gran discrecionalidad para invocarlos por el mero rechazo a los productos o servicios.
6. La incursión en sanciones administrativas por falta de cumplimiento de regulaciones.
7. La violación de normas sobre secretos empresariales, propiedad industrial e intelectual, competencia desleal o el abuso de posición dominante.
8. La violación de compromisos contractuales contraídos con terceros.
9. La dificultad en determinar correctamente la identidad digital de los consumidores y contratantes por ser relaciones en ausencia y a distancia.
10. La falta de integridad y autenticidad en las comunicaciones electrónicas.
11. La incertidumbre sobre el régimen de responsabilidad aplicable a la empresa y sus funcionarios en la era digital.
12. La inseguridad informática, los incidentes y los ataques cibernéticos.
13. Los atentados a la integridad de los negocios, el fraude informático, la injuria y la calumnia utilizando redes sociales o afectación de la reputación en línea.
14. Las regulaciones aplicables en terceros países a las actividades en línea.
15. El desconocimiento de jueces y árbitros sobre las nuevas categorías tecnológicas y la dificultad para adjudicar derechos o para que las decisiones sean aplicables. (Peña, 2014)



Para mitigar los riesgos enunciados, los administradores pueden generar, adoptar e implementar políticas de gestión y manejo de tecnología e innovación tecnológica (programas de ordenador y patentes, entre otras), programas de seguridad y aseguramiento de información, políticas de manejo adecuado de datos personales y privacidad, políticas de gestión, términos y condiciones para la contratación electrónica, políticas de gobernanza y manejo de gestión de mensajes de datos y comunicaciones electrónicas incluyendo generación, almacenamiento y transmisión y políticas de seguridad informática y de certificación digital, entre otras.

La seguridad tecnológica: el estándar de diligencia de los empresarios

La seguridad tecnológica es una obligación para todas las empresas que utilicen tecnología y que tengan información propia o de terceros que sea relevante, que tenga protección legal o valor económico. Con los mecanismos, herramientas y políticas que se planeen y adopten en relación con los sistemas de información se debe garantizar la protección y preservación de las características y cualidades de la información como la integridad, el acceso, la usabilidad, la confidencialidad, la autenticidad y el no repudio.

Además de las normas legales, existen normas de autorregulación sobre estándares de seguridad informática como la ISO 27001 que es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y que describe la manera de gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013.

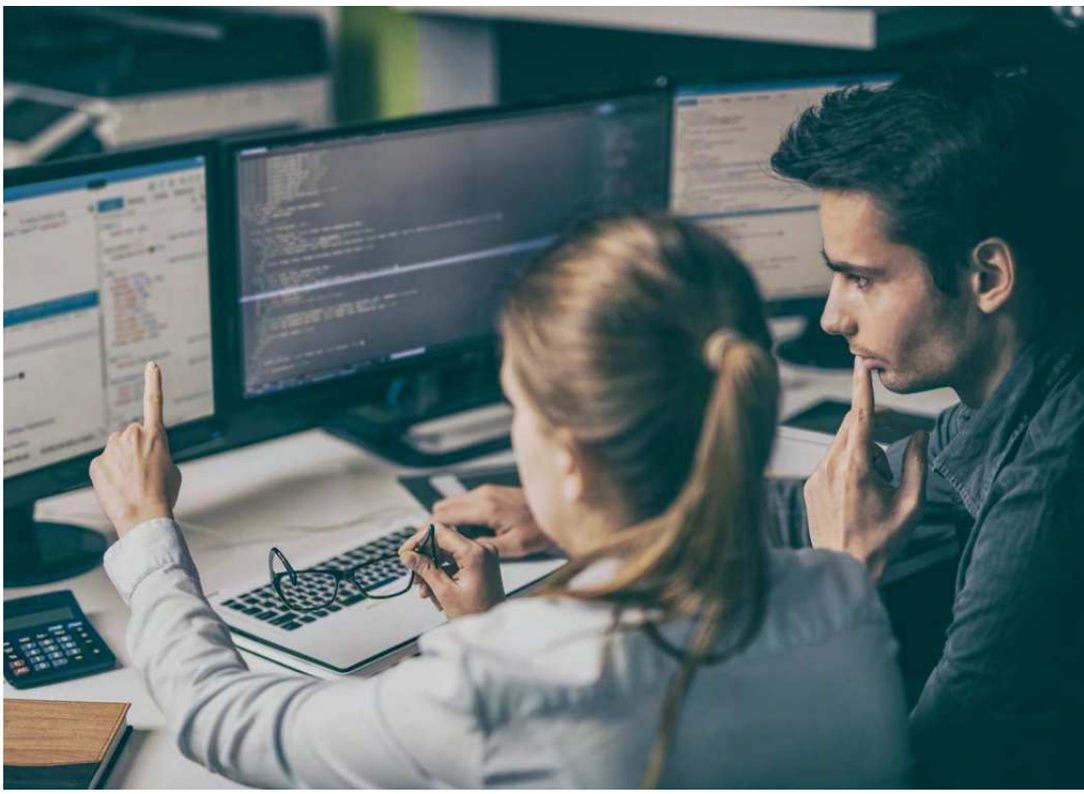
La norma ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública. Proporciona una metodología para implementar la gestión de la seguridad de la información en una organización y permite que una empresa sea certificada. De esta manera, se ha convertido en la principal norma global para la seguridad de la información.

La garantía de disponibilidad y usabilidad de la información digital puede ser utilizada para defender la posición de las empresas en procesos judiciales y administrativos. Los empleados son usuarios generadores de contenido digital, por lo que se debe reforzar su compromiso con las empresas de ser responsables respecto al contenido que publiquen en sitios web y redes sociales. En caso de que las opiniones o contenidos solo comprometan la responsabilidad de la empresa, esta consigna debe constar de manera expresa.

Hasta hace poco las herramientas informáticas y equipos eran de propiedad exclusiva de las empresas y estaban bajo un control centralizado. Sin embargo, con la tendencia de utilizar equipos personales, adquiere mayor importancia la separación de la información en el dispositivo. En este sentido, hay que dejar claridad que la información le pertenece a la empresa así el equipo sea propiedad del empleado.

Así, la seguridad informática de las organizaciones busca lograr el mayor nivel posible de confiabilidad y aseguramiento de las arquitecturas de sus sistemas de información, así como evaluar el nivel de dificultad requerido por los atacantes para ingresar y vulnerar las medidas de protección. En definitiva, se trata de comprender que la seguridad también es un asunto ligado a la tecnología y que se requiere implementar estrategias para gestionar los riesgos y mitigar sus efectos.

La seguridad tecnológica es una obligación para todas las empresas que utilicen tecnología y que tengan información propia o de terceros que sea relevante, que tenga protección legal o valor económico".



Conclusiones

1. Las empresas de todos los tamaños tienen grandes desafíos para lograr aprovechar las bondades de la transformación digital. En este

proceso de creación y adopción de nuevos conocimientos también deben detectar, prevenir y mitigar los riesgos que implica el uso de las tecnologías para sus actividades mercantiles.

2. La información, la innovación, la creación de conocimiento y la transferencia y recepción de tecnología son los paradigmas del siglo XXI que están transformando la sociedad y el ámbito empresarial. El derecho comercial asume de manera paulatina ese desafío mediante la adecuación del derecho informático, la propiedad intelectual e industrial, el derecho al emprendimiento y a la seguridad de la información, entre otros.
3. Las empresas de tecnología y del ecosistema digital tienen un grado de responsabilidad derivado de regulaciones legales a sus actividades por desempeñar el servicio público de prestación de servicios y provisión de redes TIC.
4. El régimen de responsabilidad de los administradores, por sus funciones y por la extralimitación de estas, debe diferenciar la asunción de riesgos en el marco de la innovación y la adopción de tecnologías en el curso normal de las actividades de la empresa y las actividades que impliquen ilegalidad o conductas dolosas.
5. Los datos personales son una categoría de información que tiene protección constitucional, legal y regulatoria con una amplia jurisprudencia de la Corte Constitucional y con la vigilancia de la Superintendencia de Industria y Comercio como Autoridad Nacional de Protección de Datos. Los derechos de acceso, rectificación, cancelación y oposición deben ser cumplidos so pena de que exista una sanción administrativa, indemnización de perjuicios e incluso la comisión del delito de violación de datos personales.
6. Las empresas deben definir el rol de los nuevos empleos y funciones para utilizar y explotar las nuevas herramientas informáticas y de Internet.
7. Las empresas deben adoptar políticas para el manejo y gestión de los riesgos propios de la transformación digital, sistemas de gestión y administración de la seguridad de los sistemas de información, políticas de seguridad documental, retención documental, archivo y gestión de pruebas digitales y computación forense, política de recaudo, recolección, tratamiento de datos personales, políticas y medidas tecnológicas de protección de información confidencial y política de trazabilidad de las transacciones electrónicas con los consumidores.



Referencias

Ceruzzi, P. (2003) A History of Modern Computing, MIT PRESS, Boston.

Anderson, C. (2012) Makers The New Industrial Revolution. Crown Business, Nueva York.

Rallo, A. y Martínez R. (2013) Derecho y Redes Sociales. Civitas Thomson Reuters, Madrid-

Peña, D. (2013) Responsabilidad de los Proveedores del Servicio de Internet en relación con la Propiedad Intelectual, Universidad Externado de Colombia, Bogotá.

Peña, D. (2014) Responsabilidad Jurídica en la web 2.0 y en las Redes Sociales en Anuario de Responsabilidad Civil y del Estado. Ediciones UNAULA, Medellín.