# Protección de datos

Con fecha 30 de noviembre de 2024, el Ministerio de Justicia y Derechos de Perú aprobó mediante el Decreto Supremo 016-2024-JUS un nuevo Reglamento de la Ley 29733 de Protección de Datos Personales.

El documento permitirá que el país cuente con un marco normativo moderno y sólido que garantice una adecuada tutela de los derechos de los ciudadanos frente a los riesgos generados para los datos personales a partir de las nuevas tecnologías digitales.

Entre otras cuestiones, introduce novedades relativas a las obligaciones en caso de que se den incidentes de seguridad, a la figura del Oficial de Datos Personales, a la portabilidad de los datos o a la implementación de nuevas infracciones.

El Reglamento está alineado con la Directiva Europea de Protección de Datos y entrará en vigor el 30 de marzo de 2025. Las obligaciones referidas a la designación del Oficial de Datos Personales entrarán en vigencia progresivamente a partir del 30 de noviembre de 2025, en base a las ventas anuales.

Por su parte, en Chile también se publicó recientemente la Ley 21719 que regula la Protección y el Tratamiento de los Datos Personales, tras muchos años en periodo de consulta pública.

Entre las modificaciones más destacadas se incluyen la creación de la Agencia de Protección de Datos, la asignación de mayores obligaciones a los responsables del tratamiento de datos, el fortalecimiento de los derechos ARCO de los titulares y la implementación de sanciones significativas y efectivas, que pueden alcanzar hasta 20.000 UTM (US$1.400.000 aproximadamente).

El nuevo texto de la ley entrará en vigor en un plazo de 24 meses.

---

# Ciberseguridad

El 1 de enero de 2025 entró en vigor en Chile la Ley Marco sobre Ciberseguridad.

Entre otras cuestiones, la ley crea la Agencia Nacional de Ciberseguridad como autoridad supervisora e introduce varios principios aplicables a las entidades: (i) control de daños; (ii) coordinación con la autoridad; (iii) respuesta responsable (iv) seguridad informática; (v) racionalidad; y (vi) seguridad y privacidad por defecto y desde el diseño.

La banca, los servicios financieros y los medios de pago son considerados «Servicios Esenciales», lo que les obliga a reportar a las autoridades ciberataques e incidentes de seguridad en un plazo de 3 horas; y a aplicar medidas para prevenir, reportar y resolver incidentes de seguridad. También se introducen deberes específicos para las entidades consideradas «Operadores de Importancia Vital».

Además, junto con la entrada en vigor del resto de disposiciones de la Ley se publican las normas sobre requisitos y procedimiento para el reporte de incidentes de ciberseguridad a la autoridad nacional, así como la taxonomía y clasificación de incidentes de ciberseguridad.

# Protección de datos y ciberseguridad

El Congreso chileno aprobó, tras 7 años de tramitación, el proyecto de la ley de Protección de Datos Personales que sigue los estándares establecidos en el Reglamento General de Protección de Datos de la Unión Europea y crea la Agencia de Protección de Datos con el objetivo de fiscalizar su cumplimiento y aplicar sanciones. Esta Ley, cuyo texto definitivo está pendiente de publicación, permitirá a Chile ser declarado por la Comisión Europea como país con un nivel adecuado de protección de datos personales, lo que facilitará la transferencia internacional de datos entre Chile y la Unión Europea. La nueva ley entrará en vigor 24 meses después de su publicación para adaptarse al nuevo régimen.

En la Unión Europea, por su parte, se publicó el Reglamento en el que se detallan los casos en que un incidente se considera significativo y que obliga a las entidades a notificar dichos incidentes. Destacar, entre otros, (i) que el incidente haya causado o pueda causar a la entidad pertinente pérdidas financieras directas superiores a 500.000 EUR o al 5% de su volumen de negocios total anual en el ejercicio financiero anterior, (ii) que un servicio de computación en nube esté totalmente indisponible durante más de treinta minutos, (iii) que la integridad, confidencialidad o autenticidad de los datos almacenados, transmitidos o tratados en relación con la prestación de un servicio de computación en nube se vean comprometidas como consecuencia de una acción presuntamente

malintencionada.

---

# Ciberseguridad y estrategia digital

## Ciberseguridad y delitos informáticos

En diciembre de 2023, se publicó en Chile la Política Nacional de Ciberseguridad 2023 – 2028, con el propósito de guiar las actuaciones del Estado en el ámbito de la ciberseguridad, estableciendo un plan de acción, metas y objetivos para abordar los múltiples desafíos y obstáculos que enfrenta el país en este campo (delitos cibernéticos, vulnerabilidad de las infraestructuras, entre otros).

La política se centra en las siguientes materias: 1. Infraestructura resiliente; 2. Derechos de las personas y protección de los derechos en Internet; 3. Cultura de ciberseguridad; 4. Coordinación nacional e internacional; 5. Fomento a la industria y la investigación científica.

También en Perú se publicó a finales del pasado año una modificación a la Ley de Delitos Informáticos respecto al acceso ilícito a sistemas informáticos y a la comisión de fraude informático, ampliando las multas y penas privativas de libertad aplicables para estos delitos.

Por otra parte, en febrero de 2024 el Senado en Chile aprobó las enmiendas a la Ley Marco de Ciberseguridad e Infraestructura Crítica, convirtiéndose así en el primer país de América Latina y El Caribe en tener un proyecto de tal envergadura, que define cuáles son los servicios esenciales, los operadores de instancia vital y crea la Agencia Nacional de Ciberseguridad

(ANCI).

## Estrategia Nacional Digital

En Colombia, el Ministerio de Tecnologías de la Información y las Comunicaciones dio a conocer a comienzos de febrero de 2024 la Estrategia Nacional Digital 2023 – 2026, que tiene como objetivo incentivar el potencial de la transformación digital para superar los desafíos económicos, sociales y ambientales del país, a través del aprovechamiento de los datos y el uso de tecnologías digitales para alcanzar objetivos sociales, ambientales y económicos. La estrategia se desarrollará a través de los siguientes ejes estratégicos:

Conectividad digital para cambiar vidas
Acceso, uso y aprovechamiento de datos para impulsar la transformación social
Seguridad y confianza digital para la garantía de las libertades y el desarrollo integral de las personas
Habilidades y talento digital como motor de oportunidades
Inteligencia Artificial y otras tecnologías emergentes para la generación de valor económico y social
Transformación digital pública para fortalecer el vínculo Estado – Ciudadanía
Economía digital para la transformación productiva
Sociedad digital para un desarrollo inclusivo, equitativo y sostenible

En línea con lo anterior, el Ministerio también presentó una hoja de ruta para el desarrollo y la aplicación de la inteligencia artificial: un documento estratégico que guiará el desarrollo de políticas, acciones y decisiones hacia un futuro impulsado por la tecnología, pero siempre arraigado en principios éticos y sostenibles.

---

# Finanzas abiertas

La Superintendencia Financiera publicó la Circular Externa 004 de 7 de febrero de 2024, con instrucciones relativas a finanzas abiertas y comercialización de tecnología e infraestructura. Las «finanzas abiertas» se definen como la práctica por la que las entidades abren sus sistemas para que la información de sus clientes pueda ser compartida de forma estandarizada con otras entidades vigiladas, o con terceros, con la autorización del cliente y con el objetivo de que dichas entidades provean servicios a los clientes (productos de terceros).

## Estándares de seguridad

Entre los puntos destacables del nuevo marco regulatorio se encuentran los estándares de seguridad exigidos para Terceros Receptores de Datos (TRD), tales como acreditar la certificación ISO 27001 o evidenciar que se cuenta con una política de riesgos y controles dirigida a proteger los datos personales.

## Tratamiento de datos personales

Se establecen obligaciones para proteger los datos de los consumidores financieros en estas operaciones, poniendo como foco fundamental su consentimiento previo, expreso e informado y revocable en todo momento cuando lo considere oportuno.

## Deberes de revelación de la información

Igualmente se incluyen deberes de revelación de la información por parte de los actores del sistema, a fin de que tanto las entidades financieras como los TRD implementen los canales y procedimientos necesarios para que el usuario pueda ejercer los derechos que se desprenden del otorgamiento de su consentimiento.

## Educación financiera

Finalmente, la Circular señala que las entidades deberán contar con programas de educación financiera para informar a los consumidores financieros sobre los derechos, obligaciones y responsabilidades derivados del tratamiento de sus datos.

# Plan Colmena

El pasado 27 de abril fue promulgada la Ley 297 de 27 que adopta la Estrategia denominada “Plan Colmena”, estrategia que busca crear planes de trabajo que contribuyan a cerrar las brechas sociales existentes dentro de la comunidad.

## Objetivo

Para una completa visión de esta estrategia, es necesario atender al Decreto Ejecutivo No. 244 de 16 de diciembre de 2021 por el que se instituyó el Sistema de Gestión de la Estrategia del Plan Colmena con el objetivo de crear una herramienta informática que canalizara a lo largo y ancho de la República de Panamá, toda la información necesaria para llevar a cabo esta estrategia, mediante el desarrollo de programas, acciones y proyectos para erradicar la desigualdad y la pobreza multidimensional, así como la vulnerabilidad social, dentro del territorio nacional.

## Líneas de Acción y Marco Estratégico

El marco estratégico del Plan Colmena se estructura en cuatro ejes; Desarrollo Social, Desarrollo Económico, Infraestructura y Sostenibilidad Ambiental.

Las ofertas de servicios que se reciban deberán estar orientadas a la atención de las doce principales privaciones y necesidades de los corregimientos más vulnerables del país: la atención de la primera infancia, nutrición, obtención de agua limpia y sanidad básica, salud, educación, vivienda, actividades que generen ingresos y emprendimientos para la comunidad, seguridad, deporte y cultura, conservación del medio ambiente, electrificación rural e infraestructura vial. Es indispensable la participación ciudadana, la academia, los gremios, así como las diversas organizaciones sindicales y sociales.

## Otras consideraciones

La norma establece que será responsabilidad de la Secretaría Técnica del Gabinete Social, el diseño metodológico de la Estrategia Nacional Plan Colmena, estudios, impacto, interactuando y articulando el proyecto entre las entidades de los gobiernos locales de las provincias y comarcas del país. Para su desarrollo, las entidades gubernamentales programarán los recursos que requieran para los planes, proyectos e iniciativas que atiendan las prioridades incluidas en el Plan.

Finalmente, la Ley exige a los gobernadores de cada provincia emitir reportes de seguimiento mensual, elaborar informes sobre el avance del Plan Colmena. Esta Ley será reglamentada posteriormente, mediante Resolución de Gabinete Social.

---

# Gestión de la seguridad de la información y la ciberseguridad

A fin de que las empresas fortalezcan sus capacidades de ciberseguridad y sus procesos de autenticación, la Superintendencia de Banca, Seguros y AFP ha publicado el presente Reglamento

para actualizar la normativa sobre gestión de seguridad de la información, una normativa bastante esperada y necesaria en la actualidad, aún más considerando que el único dispositivo legal sobre la materia era la Circular G-140, del año 2009.

Es complementario al Reglamento para la Gestión del Riesgo Operacional y está en línea con los estándares y buenas prácticas internacionales en esta materia. A continuación, las cuestiones más relevantes:

## Sistema de gestión de seguridad de la información y ciberseguridad

El Reglamento define el sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C) como el conjunto de políticas, procesos, procedimientos, roles y responsabilidades diseñados para identificar y proteger los activos de información, detectar eventos de seguridad, así como prever la respuesta y recuperación ante incidentes de ciberseguridad.

Establece que todas las compañías deberán contar con este sistema, que será proporcional al tamaño, la naturaleza y la complejidad de sus operaciones y se basará en los siguientes principios:

Confidencialidad: la información sólo estará disponible para entidades o procesos autorizados, incluyendo las medidas para proteger la misma
Disponibilidad: el acceso y el uso a la información deberán ser oportunos
Integridad: se deberá asegurar la irrenunciabilidad de la información y su autenticidad, y evitar su modificación o destrucción indebida

## Medidas mínimas de seguridad

El capítulo II regula el régimen general del SGSI-C: objetivos y requerimientos, alcance, actividades planificadas e intercambio de información de ciberseguridad, así como las medidas mínimas de seguridad de la información a adoptar por las empresas, entre las que se encuentran: seguridad en los recursos humanos, en las operaciones, en las comunicaciones, física y ambiental; controles de acceso físico y lógico; adquisición, desarrollo y mantenimiento de sistemas; gestión de incidentes de ciberseguridad y de activos de información; y criptografía.

## Programa de ciberseguridad

El Reglamento contempla que todas las entidades con presencia en el ciberespacio deberán contar, de manera permanente, con un programa de ciberseguridad aplicable a las operaciones, procesos y demás activos de información.

Este programa deberá prever un diagnóstico y un plan de mejora sobre sus capacidades de ciberseguridad, para lo cual tendrá que seleccionar un marco de referencia internacional sobre la materia, que le permita, como mínimo:

Identificar los activos de información
Proteger de las amenazas a los activos de información
Detectar incidentes de ciberseguridad
Responder con medidas que reduzcan el impacto de los incidentes
Recuperar las capacidades o servicios tecnológicos que pudieran ser afectados

## Responsabilidades del directorio y de la gerencia

En su artículo 5 recoge que el directorio será responsable de aprobar y facilitar las acciones requeridas para contar con un SGSI-C apropiado a las necesidades de la empresa y su perfil de riesgo,

y destaca entre sus funciones:

Aprobar políticas y lineamientos para la implementación del SGSI-C y su mejora continua
Asignar los recursos técnicos, de personal y financieros requeridos para su implementación y adecuado funcionamiento
Aprobar la organización, roles y responsabilidades para el SGSI-C, incluyendo los lineamientos de difusión y capacitación que contribuyan a un mejor conocimiento de los riesgos involucrados

Por otra parte, en el artículo 6 establece que la gerencia general será responsable de tomar las medidas necesarias para implementar el SGSI-C de acuerdo a las disposiciones del directorio y lo dispuesto en el Reglamento.

Además, que los gerentes de las unidades de negocios y de apoyo deberán favorecer el buen funcionamiento del SGSI-C y gestionar los riesgos asociados a la seguridad de la información y Ciberseguridad en el marco de sus funciones.

# Responsabilidades del comité de riesgos

Además de las funciones propias del comité de riesgos, el Reglamento le confiere las siguientes responsabilidades relativas a la seguridad de la información y a la ciberseguridad:

Aprobar el plan estratégico del SGSI-C y recomendar las acciones a seguir
Aprobar el plan de capacitación a fin de garantizar que el personal, la plana gerencial y el directorio cuenten con competencias necesarias en seguridad de la información y en ciberseguridad.
Fomentar la cultura de riesgo y conciencia de la necesidad de medidas apropiadas para su prevención

Para su cumplimiento, las empresas podrán constituir un comité especializado en seguridad de la información y ciberseguridad (CSIC). Para aquellas empresas comprendidas en el régimen simplificado que no cuenten con un comité de riesgos o un CSIC, las funciones antes indicadas serán asignadas a la gerencia general.

# La función de seguridad de la información y ciberseguridad

El Reglamento exige a las empresas implementar la función de seguridad de la información y ciberseguridad, y contar con un equipo de trabajo multidisciplinario de manejo de incidentes de ciberseguridad que esté capacitado para implementar el plan y los procedimientos para gestionarlos.

Estará conformado por representantes de las áreas que permitan prever los aspectos legales, técnicos y organizacionales, de forma consistente con los requerimientos del programa de ciberseguridad.

# Autenticación y régimen simplificado y reforzado

En la regulación también se contemplan otras cuestiones, como la implantación de procesos de autenticación, el enrolamiento del usuario en servicios provistos por canal digital, la autenticación reforzada para operaciones por canal digital, las exenciones de autenticación reforzada para operaciones por canal digital o el uso de interfaces de programación de aplicaciones para la provisión de servicios en línea.

Asimismo regula la provisión de servicios por terceros y el régimen simplificado y reforzado del SGSI-C.

## Otras modificaciones

El Reglamento modifica diversa normativa regulatoria a fin de adecuarla a las disposiciones del presente Reglamento, entre ellos: (i) Reglamentos de Auditoría Interna y Externa a fin de incluir la evaluación al cumplimiento de este sistema; (ii) Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos y Reglamento de Riesgo Operacional, para incluir definiciones y sustituir las disposiciones sobre “Bienes y/o Servicios Provistos por Terceros”; (iii) Reglamento de Tarjetas de Crédito y Débito para modificar la Información mínima, condiciones y vigencia aplicable a las tarjetas de débito; (iv) Reglamento de Operaciones con Dinero Electrónico para sustituir las disposiciones de los Soportes para uso de dinero electrónico.

## Aplicación y entrada en vigor

La normativa será de aplicación obligatoria a las empresas de operaciones múltiples, Administradoras de Fondos de Pensiones (AFP), corredoras de seguros, empresas de Seguros y/o Reaseguros (según su promedio de activos), Empresa Emisora de Dinero Electrónico, Banco de la Nación, Banco Agropecuario, COFIDE, Fondo MIVIVIENDA S.A., entre otros.

Entrará en vigor el 1 de junio de 2021, fecha en la que quedará derogada la Circular G 140- 2009, con excepción de las disposiciones listadas en los literales del artículo décimo del Reglamento, sujetos a un plazo de adecuación.

---

# Transformación digital y confianza digital

El gobierno peruano ha dictado los Decretos 006-2020 y 007-2020 en el marco de la Política Nacional de Competitividad y Productividad1 y ante la necesidad de reducir la brecha digital según lo aconsejado por el Programa de las Naciones Unidas para el Desarrollo (PNUD).

Teniendo en cuenta además, que Perú pretende formar parte de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), que reconoce que las tecnologías digitales podrían contribuir a cada uno de los Objetivos de Desarrollo Sostenible (ODS), el ejecutivo ha aprobado los siguientes Decretos:

## I. sistema Nacional de Transformación Digital. Decreto 006-2020

La norma define “Transformación Digital” como el proceso continuo, disruptivo, estratégico y de cambio cultural que se sustenta en el uso intensivo de las tecnologías digitales, sistematización y análisis de datos para generar efectos económicos, sociales y de valor para las personas.

Ante este concepto, se establece el Sistema Nacional de Transformación Digital, sistema funcional del Poder Ejecutivo conformado por un conjunto de principios, normas, procedimientos e instrumentos mediante los cuales se organizan las actividades de la administración pública y promueve las actividades del sector privado orientadas a alcanzar los objetivos del país en materia de transformación digital.

Tal y como establece la norma, los cuatro fines perseguidos por este Sistema son:

Fomentar la transformación digital y el uso efectivo de tecnologías digitales.
Impulsar la innovación digital y el fortalecimiento de una sociedad digital inclusiva, esto es, ciudadanía con derechos y deberes digitales.
Promover la economía digital, competitividad, productividad e inclusión financiera.
Fortalecer el acceso e inclusión a las nuevas tecnologías digitales y la confianza digital a través de seguridad, transparencia, protección de datos personales y gestión ética.

Asimismo se indica que las entidades del sector privado considerarán en sus acciones los objetivos de la Política y Estrategia Nacional de Transformación Digital -pendientes de publicación- y que se encuentran orientadas a fortalecer la confianza digital en el diseño e implementación de servicios digitales.

# II. Marco de Confianza Digital y medidas para su fortalecimiento. Decreto 007-2020

Esta norma tiene establece las medidas necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el Perú.

A estos efectos, define la “Confianza Digital” como el estado que emerge resultado de cuán veraces, predecibles, éticas, transparentes, seguras, inclusivas y confiables son las interacciones digitales que se generan entre personas, empresas, entidades públicas o cosas en el entorno digital.

Atendiendo a esta Confianza Digital, se crea el Marco de Confianza Digital compuesto por tres ámbitos: Protección del consumidor, transparencia y Seguridad digital; y que la norma define como el conjunto de principios, políticas, procesos, personas, empresas, entidades públicas, tecnologías y estándares mínimos que permiten asegurar y mantener la confianza en el entorno digital.

La norma reconoce como medidas de fortalecimiento las siguientes:

Creación del Centro Nacional de Seguridad Digital.- Plataforma digital que gestiona, dirige y supervisa la operación y promoción de la Seguridad Digital (SD) y que es el responsable de identificar, detectar, proteger y recuperar información sobre incidentes de SD.
Registro Nacional de Incidentes de SD.- Recibe, consolida y mantiene datos e información sobre los incidentes de SD reportados por los Proveedores de servicios digitales en el que puedan servir de evidencia o insumo para su análisis, investigación y solución.
Definición y delimitación de “Proveedor de Servicios Generales”.- Comprende a cualquier entidad pública u organización del sector privado, independientemente de su localización geográfica, que sea responsable por el diseño, prestación y/o acceso a servicios digitales en Perú. Entre las obligaciones establecidas están las de notificar al CNSD todo incidente de SD; implementar medidas de seguridad (física, legal, técnica) para garantizar la confidencialidad de la información en los servicios brindados; o reportar y colaborar con el Ministerio de Justicia, entre otros.
Creación del Centro Nacional de Datos.- Plataforma digital que gestiona, dirige y supervisa la operación, educación, promoción, colaboración y cooperación de datos a fin de fortalecer la confianza y bienestar de las personas. De hecho, la norma reconoce a los Datos como activos estratégicos, debiendo todas las entidades públicas y privadas administrarlos garantizando que estos sean tratados por durante el tiempo que sea necesario y cuando sea apropiado.

Estas normas suponen los primeros pasos del Gobierno para impulsar la transformación digital, si bien todavía queda mucho por hacer para determinar el contenido y el alcance de los reglamentos y políticas que se generen a partir de las citadas normas.

1 Fue aprobada en diciembre de 2018 y presenta un conjunto de medidas consensuadas entre el sector público y privado encaminadas a establecer un entorno favorable y competitivo sobre la base de un crecimiento económico sostenible

---

# Tecnologías financieras y transformación digital

Teniendo en cuenta el contexto actual y la revolución tecnológica en que vivimos, el Congreso y Gobierno de Colombia han implementado distintas medidas para regular las últimas innovaciones en tecnología financiera y reducir la brecha digital.

En este sentido cabe destacar en primer lugar, el Proyecto de Ley 063 de 2019, que tiene como fin la promoción del uso de las Sociedades Especializadas en Depósitos y Pagos Electrónicos (SEDPEs), entendidas como nuevas tecnologías financieras, mejorando y ampliando de esta manera la provisión de microcréditos a sectores productivos. Es decir, las SEDPEs otorgarán créditos a través de plataformas digitales fomentando la inclusión financiera por un lado y reduciendo las brechas de desigualdad regional, ampliando la oferta en los servicios de financiación.

Por otro lado, la Superintendencia Financiera de Colombia (SFC) ha emitido la Circular Externa 029 de 2019, que contiene instrucciones precisas para las entidades vigiladas relacionadas con requerimientos mínimos de seguridad y calidad en la realización de operaciones, información al consumidor financiero y uso de factores biométricos.

Estas nuevas instrucciones implican el fortalecimiento del uso de canales digitales para la prestación de servicios financieros en condiciones de seguridad y con apego a estándares internacionales en la materia.

Los aspectos regulados por la Circular son los siguientes:

Gran abanico de posibilidades existentes para mejorar la prestación de servicios financieros ofrecidos por las entidades vigiladas a los consumidores y optimizar sus procesos: realidad aumentada, internet de las cosas, blockchain, inteligencia artificial, machine learning, big data, robots, entre otras.
Requerimientos mínimos para la implementación y uso de biometría como factor de autenticación electrónica.
El deber de las entidades de establecer los parámetros a partir de los cuales se requerirán mecanismos fuertes de autenticación para las transacciones realizadas mediante la utilización de los medios de pago (tarjetas débito) con o sin contacto.
La posibilidad que tienen las Entidades para que la información actualizada de los productos, canales, puntos de atención, servicios y tarifas, sea puesta a disposición de terceros desarrolladores de API (Application Programming Interface).

Por último, el Gobierno ha elaborado la Política Nacional para la transformación digital e inteligencia artificial para potenciar la generación de valor social y económico en el país a través del uso estratégico de tecnologías digitales en el sector público y el sector privado, impulsando la productividad y favoreciendo el bienestar de los ciudadanos.

Esta Política aborda los retos específicos de la transformación digital, así como de la conectividad, y

permite reducir la brecha digital entre zonas rurales y zonas urbanas.

Entre los aspectos más destacados de la Política, los cuales han sido denominados por el Gobierno como planes de acción, se encuentran los siguientes:

Disminución de barreras relacionadas con la falta de cultura y el desconocimiento ante la transformación digital en el sector privado.
Desarrollo y ajustes normativos e institucionales para favorecer la adopción de la transformación digital en componentes clave de la productividad empresarial.
Ejecución de iniciativas de alto impacto apoyadas en la transformación digital.

Esta política contribuirá a la generación de las redes de conectividad rural que hasta ahora constituyen un barrera para el acercamiento de los servicios financieros al sector rural del país.

---

# Actualización de las medidas europeas sobre ciberseguridad

El 27 de junio entró en vigor el Reglamento de la Unión Europea del Parlamento Europeo relativo a la Agencia de la Unión Europea para la Ciberseguridad y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación.

La norma, que deroga el anterior Reglamento sobre la Ciberseguridad del 2013, tiene como aspiración alcanzar un nivel elevado de ciberseguridad, ciberresiliencia y confianza dentro de la Unión Europea.

A continuación destacamos los dos bloques fundamentales del documento:

## Agencia Europea para la Ciberseguridad

En primer lugar, el Reglamento establece los objetivos y aspectos organizativos de la nueva Agencia Europea para la Ciberseguridad (ENISA), y le asigna las siguientes tareas:

Contribuir a la elaboración y ejecución de la política y del derecho de la Unión en el ámbito de la ciberseguridad
Asistir a los Estados en la creación de capacidades de ciberseguridad
Apoyar la cooperación entre los países miembros, las instituciones, órganos y organismos de la Unión y entre las partes interesadas
Promover el desarrollo y la aplicación de la política de la UE en materia de certificación de la ciberseguridad de productos, servicios y procesos TIC
Analizar las tecnologías emergentes y preparar evaluaciones sobre los efectos esperados, de tipo social, jurídico, económico y reglamentario, de las innovaciones tecnológicas
Sensibilizar al público sobre los riesgos relacionados con la ciberseguridad y facilitar orientaciones sobre buenas prácticas
Asesorar a las instituciones, órganos y organismos de la Unión y a los Estados miembros sobre las necesidades y prioridades de la investigación en el ámbito de la ciberseguridad y las tecnologías de la información, y a utilizar eficazmente las tecnologías de prevención del riesgo
Promover la cooperación internacional en relación con los problemas que se refieren a la

ciberseguridad

## Certificación de la ciberseguridad

Por otra parte, aborda la definición de un marco para la creación de esquemas europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de las tecnologías de la información y la comunicación (TIC) y de crear un mercado único digital para estos productos, servicios y procesos.

Este marco define un mecanismo destinado a instaurar esquemas europeos de certificación de la ciberseguridad y a confirmar que los productos, servicios y procesos de TIC que hayan sido evaluados con arreglo a dichos esquemas, cumplen los requisitos de seguridad especificados. De esta manera se trata de proteger la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o las funciones o servicios que ofrecen.

La Comisión Europea publicará un programa de trabajo evolutivo para los esquemas europeos de certificación que definirá las prioridades estratégicas para los futuros esquemas e incluirá una lista de productos, servicios y procesos de TIC, o de categorías de los mismos, que pudieran beneficiarse de su inclusión en el ámbito de aplicación de un esquema europeo de certificación de la ciberseguridad.

---

# Modificación del reglamento de gestión de conducta de mercado

Con la finalidad de incorporar disposiciones y establecer precisiones que permitan el desarrollo de la oferta de productos y servicios financieros en un entorno digital, así como adecuar el alcance del marco normativo vigente considerando los productos y servicios ofrecidos por las empresas, al tamaño y volumen de sus operaciones, la Superintendencia de Banca, Seguros y AFP (SBS) publicó el pasado mes de octubre la modificación del Reglamento de Gestión de Conducta de Mercado del Sistema Financiero, del Reglamento de Auditoría Interna, Reglamento de Tarjetas de Crédito y Débito, del Manual de Contabilidad para las empresas del Sistema Financiero y de la Circular G-184-2015 sobre el Servicios de Atención al Usuario.

## Mecanismos de seguridad

Con las modificaciones introducidas al Reglamento de Gestión de Conducta de Mercado del Sistema Financiero se busca que las empresas del sistema financiero incrementen sus mecanismos de seguridad, para lo cual deberán utilizar algún factor de autenticación con el fin de validar la identidad del cliente y dejar constancia de la aceptación. Además, las empresas deberán acreditar la entrega al cliente, por cualquier medio, del número de la resolución mediante el cual la SBS aprobó las cláusulas generales correspondientes al contrato celebrado.

## Comunicación con el cliente

Por otra parte, la norma faculta a las empresas a utilizar medios de comunicación físicos o electrónicos con el cliente y deberán contar con canales de fácil acceso para que los clientes puedan resolver el contrato, debiendo como mínimo contar con los mismos canales disponibles para la contratación.

## Otras modificaciones

La resolución modifica igualmente el Reglamento de Bancos de Inversión para eximirlo del Reglamento de Gestión de Conducta de Mercado, considerando la naturaleza de sus productos y clientes. Además, con la publicación de la Circular G-184-2015, se incluye en el Reporte Regulatorio los reclamos recibidos a través de canales directos o en asociación con el gremio.

---

# Nuevas disposiciones en materia de información no financiera y diversidad

Han pasado cuatro años desde que se publicara en el Diario Oficial de la Unión Europea la Directiva 2014/95/UE de 22 de octubre de 2014, en materia de divulgación de información no financiera y sobre diversidad por grandes empresas y determinados grupos empresariales. Una norma de gran relevancia que, como ya indicamos en pasadas ediciones de Progreso 13, tenía como objetivo mejorar la transparencia y la sostenibilidad de las entidades y aumentar la confianza de los inversores, los consumidores y la sociedad en general.

En noviembre de 2017 se aprobó el Real Decreto-ley 18/2017 y un año después ha sido el turno de este proyecto de ley, para transponer definitivamente al ordenamiento jurídico español la Directiva europea y situar a España a la vanguardia de la transparencia empresarial.

El Proyecto modifica el Código de Comercio, la Ley de Sociedades de Capital y la Ley de Auditoría de Cuentas, y plantea asimismo ciertas reformas a la Ley de Instituciones de Inversión Colectiva, contempladas en la Disposición adicional primera.

Si bien el contenido del Proyecto se asemeja al del Decreto-ley, la nueva norma introduce disposiciones que no estaban contempladas con tanto detalle en este último ni en el texto comunitario:

## Estado de información no financiera

Además de establecer qué sociedades están obligadas a incluir en su informe de gestión el estado de información no financiera, el proyecto completa el contenido del mismo:

Una breve descripción del modelo de negocio del grupo, incluyendo su entorno empresarial, su organización y estructura, el mercado en que opera, sus objetivos y estrategias, y los principales factores y tendencias que pueden afectar a su futura evolución
Una descripción de las políticas aplicadas por el grupo, especialmente los procesos de debida diligencia empleados para identificar, evaluar, prevenir y atenuar los riesgos e impactos significativos, incluyendo las medidas adoptadas
Los resultados de dichas políticas, debiendo incorporar indicadores clave de resultados no financieros que permitan realizar un seguimiento y una evaluación de los progresos y favorezcan la comparabilidad entre sociedades y sectores
Los principales riesgos vinculados a las actividades del grupo, explicando los procedimientos para identificarlos y evaluarlos e incluyendo además información sobre los impactos detectados, con un

desglose de los mismos y de los principales riesgos a corto, medio y largo plazo
Indicadores clave de resultados no financieros en relación a la propia actividad empresarial, que cumplan con los criterios de comparabilidad, materialidad, relevancia y fiabilidad, utilizando para ello estándares que sean generalmente aplicados y cumplan las directrices de la Comisión Europea y del *Global Reporting Iniciative*. Los resultados no financieros se deberán aplicar a cada uno de los apartados del estado de información no financiera

La norma incluye además que el estado de información no financiera consolidado deberá incluir información significativa sobre: i) cuestiones medioambientales (contaminación, economía circular y prevención y gestión de residuos, uso sostenible de los recursos, cambio climático y protección de la biodiversidad); ii) cuestiones sociales y relativas al personal (empleo, organización del trabajo, salud y seguridad, relaciones sociales, formación, accesibilidad universal de personas con discapacidad e igualdad); iii) el respeto de los derechos humanos; iv) la lucha contra la corrupción y el soborno; y v) cuestiones sobre la sociedad (compromisos de la empresa con el desarrollo sostenible, subcontratación y proveedores, consumidores, información fiscal).

Añade también que el informe de gestión deberá ser puesto a disposición del público de forma gratuita y será fácilmente accesible en el sitio web de la sociedad dentro de los seis meses posteriores a la fecha de finalización del año financiero y por un periodo de cinco años.

## Nuevas responsabilidades del consejo de administración

El proyecto incluye como nuevas responsabilidades del consejo de administración:

Velar por que los procedimientos de selección favorezcan la diversidad de edad, género, formación y experiencia profesional, y faciliten la selección de consejeras en un número que permita alcanzar una presencia equilibrada de hombres y mujeres
Supervisar el proceso de elaboración y presentación de la información financiera y del informe de gestión, que incluirá en su caso el estado de información no financiera, a fin de salvaguardar su integridad

## Informe anual de gobierno corporativo

La norma precisa también que el informe anual de gobierno corporativo que deben publicar las sociedades de capital deberá contener una descripción de la política de diversidad aplicada en relación con el consejo de administración y sus comités de apoyo, y del órgano de dirección, incluyendo: objetivos, medidas adoptadas y forma de aplicarlas, procedimientos para incluir en el consejo un número de mujeres que fomente la presencia equilibrada de mujeres y hombres en este órgano, y los resultados en el periodo de presentación de los informes. Si no existiera tal política de diversidad, las entidades deberán ofrecer explicaciones claras y motivadas al respecto.

Las sociedades también deberán incluir en este informe anual si han informado a los accionistas sobre los criterios y objetivos de diversidad, en caso de elección o renovación de miembros del consejo, de los comités o de la dirección.

## Aplicación

Las modificaciones introducidas por la Ley se aplicarán para los ejercicios económicos iniciados a partir del 1 de enero de 2018, a aquellas sociedades que formulen cuentas consolidadas y reúnan los siguientes requisitos:

Tener un número medio de trabajadores empleados por las sociedades del grupo durante el ejercicio superior a 500,

Ser consideradas entidades de interés público conforme a la legislación de auditoría de cuentas o bien reunir, durante dos ejercicios consecutivos y a la fecha de cierre de cada uno de ellos, al menos dos de las siguientes circunstancias:
Un total de partidas del activo consolidado superior a 20 millones de euros
Un importe neto de la cifra anual de negocios consolidada superior a los 40 millones de euros
Un número medio de trabajadores empleados durante el ejercicio superior a 250

Tres años después de la entrada en vigor de la norma, la obligación de presentar el estado de información no financiera consolidado, será de aplicación a todas aquellas sociedades con más de 250 trabajadores que, o bien sean consideradas de interés público conforme a la legislación de auditoría de cuentas, o bien reúnan, durante dos ejercicios consecutivos y a la fecha de cierre de cada uno de ellos, al menos una de estas circunstancias:

Un total de las partidas del activo superior a 20 millones de euros
Un importe neto de la cifra anual de negocios superior a los 40 millones de euros

---

# Recomendaciones sobre externalización a proveedores de servicios en la nube

A finales del 2017, la Autoridad Bancaria Europea (EBA, por sus siglas en inglés) publicó un informe final con un conjunto de recomendaciones relativas a la externalización de servicios en la nube por parte de las instituciones financieras, en concreto, por entidades de crédito, empresas de inversión y las autoridades competentes.

Las recomendaciones se han desarrollado basándose en las Directrices sobre *outsourcing** del Comité de Supervisores Bancarios Europeos (CEBS, por sus siglas en inglés), y tratan de dar una orientación adicional a aquellas entidades que externalizan sus actividades a proveedores de servicios en la nube, para que tomen medidas razonables para evitar riesgos operacionales indebidos.

Serán aplicables atendiendo al principio de proporcionalidad, esto es, en consideración al tamaño, la estructura y el entorno operacional en el que actúen las entidades, así como a la naturaleza, la escala y la complejidad de sus actividades.

El informe trata seis áreas clave: i) el derecho de acceso; ii) la seguridad de los datos y sistemas; iii) la ubicación de los datos y el procesamiento de datos; iv) el derecho de auditoría; v) la externalización de cadenas, y vi) los planes de contingencia y las estrategias de salida. A continuación desatacamos las cuestiones más relevantes:

## Evaluación de la materialidad

Antes de realizar la externalización de las actividades, la autoridad europea recomienda que las instituciones evalúen la materialidad de las mismas, teniendo en cuenta:

Su perfil de riesgo (por ejemplo, si son críticas para la continuidad o viabilidad de la institución y para el cumplimiento de sus obligaciones con sus clientes)
El impacto operacional de cualquier interrupción de la externalización, y los riesgos legales y

reputacionales inherentes
El impacto que cualquier disrupción de la actividad podría tener en las perspectivas de ingresos de la institución
El potencial impacto que una infracción de la confidencialidad o la falta de integridad de los datos podría tener en la institución y sus clientes

Las instituciones financieras deberán informar al órgano supervisor sobre qué actividades materiales serán externalizadas a proveedores de servicios en la nube, proporcionando datos sobre el nombre del proveedor y la compañía, las actividades que serán externalizadas, en qué fecha, la ley aplicable, entre otros. Dicha autoridad estará facultada para solicitar cualquier información adicional que considere.

Además, deberán mantener un registro actualizado con información sobre todas aquellas actividades materiales y no materiales que han sido externalizadas a proveedores de servicios en la nube, tanto a nivel individual como a nivel grupo.

# Derechos de acceso y de auditoría

Las recomendaciones recogen que las disposiciones contractuales entre la institución financiera y el proveedor de servicios en la nube deberán garantizar el pleno acceso, tanto de los supervisores competentes como de la propia entidad y su auditor, a los locales, dispositivos, sistemas, redes y datos de los proveedores, necesarios para proporcionar los servicios subcontratados (derecho de acceso).

Además, también deberán conferirle los derechos de inspección y auditoría sin restricciones, en relación con los servicios subcontratados (derecho de auditoría).

El efectivo ejercicio de estos derechos no deberá verse obstaculizado o limitado por acuerdos contractuales. Así, en caso de que la realización de auditorías pueda crear un riesgo para el entorno de otro cliente, deberán acordarse formas alternativas para proporcionar un nivel de seguridad similar al requerido por la institución.

Se proponen medidas como la posibilidad de hacer una auditoría entre varios clientes que compartan los servidores o que el proveedor aporte certificaciones de terceros, a efectos de poder ejercer el derecho de acceso a las instalaciones del proveedor y de hacer auditorías con el menor inconveniente posible para ambas entidades.

# Seguridad de datos y sistemas

Una cuestión relevante son las medidas de seguridad que deben adoptar los proveedores de servicios en la nube para proteger la confidencialidad de la información transmitida por la institución financiera, por ser claves para la gestión del riesgo operacional. En este sentido, antes de externalizar las actividades, las instituciones deberán:

Identificar y clasificar sus actividades, procesos, datos y sistemas en función de la protección requerida;
Realizar una selección exhaustiva, basada en el riesgo, de las actividades, procesos, datos y sistemas que se estén considerando externalizar;
Definir y decidir sobre el nivel adecuado de protección de la confidencialidad de los datos, la continuidad de las actividades externalizadas y la integridad y rastreabilidad de los datos y sistemas en el contexto de la externalización prevista.

Además, deberán asegurar que todas esas medidas se recojan en un acuerdo por escrito con el proveedor de servicios. Así mismo, deberán realizar un seguimiento del desempeño de las actividades

y las medidas de seguridad, de los incidentes generados y, en su caso, de las medidas correctivas implantadas.

## Ubicación y procesamiento de datos

La EBA recomienda a las instituciones actuar con especial diligencia cuando se planteen celebrar acuerdos de externalización de servicios fuera del Espacio Económico Europeo, debido a los potenciales riesgos de protección de datos y de supervisión que pudieran existir.

Así, la autoridad bancaria recomienda que las entidades realicen un análisis sobre el impacto de los potenciales riesgos, incluidos los riesgos legales y los problemas en caso de incumplimiento, así como las limitaciones de supervisión en los países donde se presten los servicios subcontratados y donde estén almacenados los datos. La evaluación deberá también incluir consideraciones sobre la estabilidad y seguridad política de las jurisdicciones en cuestión; las leyes vigentes (especialmente sobre protección de datos); y, entre otras, las disposiciones legales en materia de insolvencia que se aplicarían en caso de fallo por parte del proveedor de servicios en la nube. Todos estos riesgos deberán mantenerse dentro de los límites aceptables, y ser acordes con la materialidad de la actividad externalizada.

## Externalización en cadena

Las recomendaciones incluyen requisitos específicos para mitigar los riesgos asociados con la externalización en cadena, esto es, en los casos en los que el proveedor de servicios en nube subcontrata elementos del servicio a otros proveedores. Así, dicha externalización será posible siempre y cuando no se vean afectados los servicios ni se incumplan las obligaciones que el proveedor hubiera formalizado inicialmente con la institución financiera.

En todo caso, la institución financiera deberá revisar y hacer un seguimiento del conjunto de la actividad contratada, independientemente de si se lleva a cabo por el proveedor de servicios en la nube o por otro proveedor subcontratado.

## Planes de contingencia y estrategias de salida

Finalmente, la EBA recomienda que las instituciones planifiquen e implementen planes de contingencia y estrategias de salida bien definidas para mantener la continuidad de su negocio, en caso de que la prestación de servicios por parte del proveedor falle o se deteriore hasta niveles inaceptables.

La autoridad europea también orienta a las instituciones sobre los contenidos de los acuerdos contractuales y organizativos en relación con dichos planes y las estrategias.

## Aplicación

Las recomendaciones serán de aplicación a partir del 1 de julio de 2018.

* Todo acuerdo entre una institución financiera y un proveedor de servicios, donde el proveedor realiza un proceso, servicio o una actividad que de otra manera sería realizada por la propia institución financiera.

# Obligaciones de información para empresas de servicios de inversión

El 29 de noviembre de 2017 la Comisión Nacional del Mercado de Valores (CNMV) publicó la circular sobre obligaciones de publicidad para las empresas de servicios de inversión en materia de gobierno corporativo y política de remuneraciones.

La regulación contempla en las normas primera y segunda la información que dichas empresas deben publicar en sus páginas web, en línea con lo establecido en el artículo 185.5 del texto refundido de la Ley del Mercado de Valores y en el artículo 31 ter del Real Decreto 217/2008, de 15 de febrero, sobre régimen jurídico de las empresas de servicios de inversión y de las demás entidades que prestan servicios de inversión (RD 217/2008).

## Gobierno corporativo y política de remuneraciones

Las entidades deberán incluir en su página web la siguiente información:

Estatutos sociales
Órganos de gobierno: composición y categorías; reglamentos y normas de organización del consejo y los comités; identificación cargos de presidente del consejo y consejero delegado; comités del consejo y funciones atribuidas
Procedimientos para asegurar la idoneidad de los consejeros, directores generales y asimilados, y mecanismos para cumplir con las normas sobre incompatibilidades
Identificación si los nombramientos de los miembros del consejo y directores generales o asimilados se han adoptado o no con el informe favorable del comité de nombramientos
Estructura organizativa, líneas de responsabilidad, reparto de funciones, y criterios para prevención de conflictos de interés
Descripción de los procedimientos para identificar, medir, gestionar, controlar y comunicar internamente los riesgos a los que se expone la entidad
Descripción de los mecanismos de control interno de la entidad, incluyendo los administrativos y contables
Remuneración total devengada en cada ejercicio económico por los consejeros, reflejando la cifra total de la remuneración devengada y un desglose individualizado indicando componentes fijos y dietas, y componentes variables

En relación a este último punto, las empresas informarán de cualquier concepto retributivo devengado, cualquiera que sea su naturaleza o la entidad que lo satisfaga, y se incluirán aquellas retribuciones devengadas por pertenencia a consejos en otras sociedades del grupo o participadas en las que actúe en representación del grupo.

Se prevé que alternativamente puedan informar de la política de remuneraciones a través de un enlace directo al documento "*Información sobre Solvencia"* al que se refiere el artículo 191 de la Ley del Mercado de Valores.

## Configuración de las páginas web

La información publicada deberá recogerse de forma completa, clara, comprensible y actualizada, y ser accesible desde la página de inicio en un apartado que se denomine "*Gobierno corporativo y*

*política de remuneraciones".*

No obstante, se contempla la posibilidad de publicar la información a través de enlaces directos si esta ya se hubiera divulgado en otros apartados de la página o si fuera ofrecida de forma gratuita en las bases telemáticas de la CNMV u otros organismos.

El contenido informado deberá estar a un máximo de tres *clics* de navegación y se presentará de forma estructurada y jerarquizada. Los títulos deberán ser claros, concisos y significativos, y el lenguaje adecuado, evitando en la medida de lo posible el uso de tecnicismos y abreviaturas. En caso de ofrecer versiones para distintas plataformas, sus contenidos y presentación deberán ser homogéneos.

Además, las entidades deberán garantizar en todo momento la seguridad de la página web, así como asegurar la autenticidad y exactitud de la información, el acceso gratuito a la misma y la posibilidad de que los documentos sean descargables e imprimibles.

## Activos intangibles

Por otra parte, se recoge en la Disposición Adicional la modificación de la Circular 7/2008, sobre normas contables, cuentas anuales y estados de información reservada de las empresas de servicios de inversión y las sociedades gestoras de vehículos de inversión colectiva y gestoras de entidades de capital-riesgo.

En concreto, hace referencia al nuevo tratamiento contable de los activos intangibles, estableciendo que pasarán a considerarse activos de vida útil definida y que, por tanto, serán objeto de amortización. Si su vida útil no pudiera estimarse de forma fiable, el periodo de amortización será de 10 años.

---

# Fortalecimiento a la Protección de los Consumidores

La Constitución Política del Perú establece en el artículo 65 que el Estado defiende el interés de los consumidores y usuarios garantizando el derecho a la información sobre los bienes y servicios que se encuentran a su disposición en el mercado, en ese sentido, se aprobó la Política Nacional de Protección y Defensa del Consumidor (en adelante, Política Nacional), cuyo objetivo es el de contribuir a un mayor y más eficaz nivel protección de los derechos de los consumidores con equidad y con mayor incidencia en los sectores de consumidores más vulnerables.

Esta Política Nacional es de obligatorio cumplimiento por todas las entidades del Estado peruano, en todos los niveles de gobierno, en el marco de sus competencias.

La norma establece los siguientes objetivos específicos:

> a) Fortalecer la educación de los agentes del mercado (consumidores y proveedores) en relación a los derechos de los consumidores y su obligatorio cumplimiento, implementando las actividades dirigidas a la orientación de los consumidores en el ejercicio de sus derechos y

difusión de los mismos.

b) Garantizar la seguridad de los consumidores en el marco de las relaciones de consumo.

c) Implementar mecanismos de prevención y solución de conflictos de consumo entre proveedores y consumidores.

d) Fortalecer el Sistema Nacional Integrado de Protección del Consumidor.

Asimismo, esta Política Nacional se encuentra estructurada sobre la base de cuatro ejes de política, que responden a los objetivos específicos:

Eje de Política 1: Educación, orientación y difusión
Eje de Política 2: Protección de la salud y seguridad de los consumidores
Eje de Política 3: Mecanismos de prevención y solución de conflictos entre proveedores y consumidores
Eje de Política 4: Fortalecimiento del Sistema Nacional Integrado de Protección del Consumidor

Finalmente, se establece que el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi), en su calidad de Autoridad Nacional de Protección del Consumidor, será el encargado de coordinar la implementación de la Política Nacional.

---

# Gestión de interrupciones de servicios financieros

La Superintendencia Financiera de Colombia (SFC) expidió la Circular Externa 028 de 2016, modificada posteriormente mediante la presente Circular, mediante la cual impartió instrucciones a los establecimientos de crédito en el siguiente sentido: i) el suministro de información a los consumidores financieros y a la propio autoridad de supervisión cuando se presenten eventos que generen interrupciones en la prestación de los servicios y que impiden la realización de sus operaciones, y ii) la puesta a disposición de  los consumidores financieros de canales alternativos para dichas situaciones y mecanismos que garanticen el efectivo ejercicio de sus derechos.

En lo que tiene que ver con los canales y mecanismos de seguridad, estas instrucciones establecen que los establecimientos de crédito deberán adoptar medidas para garantizar un nivel mínimo de prestación de servicios cuando los canales sean operados fuera de línea.

Asimismo, se ha establecido que los establecimientos de crédito deberán enviar a la SFC un informe trimestral sobre la disponibilidad mensual de los canales. Este informe deberá incluir el detalle de la metodología utilizada por cada entidad para el cálculo de la disponibilidad de sus canales.

De igual manera, se establece la obligación de informar a la SFC de eventos que afecten significativamente la confidencialidad, disponibilidad o integridad de la información de los sistemas que operan los canales.

Por su parte, en relación con la información que debe ser remitida a los consumidores financieros, las instrucciones de la SFC señalan que se deberá informar a aquéllos con 8 días hábiles de antelación los

canales y servicios afectados, limitación de transacciones, canales alternativos y lapsos de interrupción, cuando se trate de situaciones previsibles, tales como ventanas de mantenimiento, entre otras.

Cuando el aviso no sea posible enviarlo con dicha antelación debido a la necesidad de realizar modificaciones y/o actualizaciones a los sistemas en un término menor, la información deberá ser enviada en el menor término que le sea posible al establecimiento de crédito, sin afectar las mencionadas modificaciones y/o actualizaciones técnicas o tecnológicas.

Adicionalmente, en caso de interrupción de algún canal por más de 1 hora, los establecimientos de crédito deberán informar a los consumidores financieros de los canales afectados, las operaciones que no se pueden realizar, los canales alternativos, la fecha y hora estimada para el restablecimiento del servicio del canal, y demás información relevante.

Finalmente, estas instrucciones señalan que los establecimientos de crédito deberán establecer mecanismos de compensación de los inconvenientes por la interrupción del servicio, que deberán incluir como mínimo aspectos sobre: i) pago de cuota de manejo y otros servicios, ii) pago por transacciones en los canales alternativos; iii) pago de intereses moratorios y reporte a centrales de información, iv) medidas para evitar afectación por imposibilidad de realizar pagos oportunos; v) canales para presentación de peticiones, quejas y reclamos.

---

# Requerimientos mínimos de seguridad

La Superintendencia Financiera de Colombia (SFC) ha publicado el proyecto normativo a través del cual busca actualizar los requerimientos mínimos de seguridad y calidad para la realización de operaciones, así como incluir los conceptos de «ambiente de venta presente», «ambiente de venta no presente» y «administradores de pasarelas de pago o procesadores de pago».

Con estas nuevas instrucciones se pretende fijar los requerimientos mínimos de seguridad que deben cumplir los establecimientos de crédito y las administradoras de sistemas de pago de bajo valor para la realización de operaciones en ambiente de venta no presente que se vinculen a establecimientos de comercio o a administradores de pasarelas o procesadores de pago.

En relación con las nuevas definiciones, este proyecto señala que por “ambiente de venta presente” se entiende aquél en el que el consumidor financiero y el proveedor de bienes y/o servicios se encuentran físicamente presentes durante la realización de la transacción comercial respectiva. En este caso, los datos de la operación se toman a través de la tarjeta de crédito, débito o a través del dispositivo electrónico que las aloje.

En cuanto a la definición de “ambiente de venta no presente”, se establece que es aquél en el que el consumidor financiero y el proveedor de bienes y/o servicios no interactúan físicamente durante la transacción comercial.

Finalmente, los “administradores de pasarelas de pago o procesadores de pago” se definen como las entidades que prestan servicios de aplicación de comercio electrónico para almacenar, procesar y/o transmitir el pago correspondiente a operaciones de venta en línea en ambiente de venta no presente.

Por otra parte, sobre los requisitos mínimos de seguridad, se establecen aspectos relativos a: i) análisis de vulnerabilidades, ii) medios de comunicación, y iii) mecanismos de autenticación.

Se establece que los tres conceptos de venta han de ser efectuados por parte de entidades supervisadas que permitan la ejecución de órdenes electrónicas para la transferencia de fondos, la compra, venta o transferencia de títulos valores y la emisión de pólizas de seguros, por sistemas de acceso remoto para clientes, Internet o dispositivos móviles.

En cuanto a los medios de comunicación, se adicionan la mensajería instantánea o cualquier otra modalidad de comunicación a través de la cual se pueda realizar el envío de información confidencial a los consumidores financieros.

Para los mecanismos de autenticación, el proyecto normativo señala que, en el caso de uso de cajeros automáticos y datáfonos, se deberá emplear alguno de los mecanismos de autenticación fijados en la norma, salvo en los casos de tarjetas que no estén obligadas a cumplir el estándar EMV (chip), caso en el cual se debe establecer un segundo factor de autenticación. Para las operaciones realizadas en internet, por su parte, se deberá dar aplicación de mecanismos de autenticación fuertes. Finalmente, se señala que el canal Banca Móvil podrá ser utilizado a través de aplicaciones de dispositivos móviles (apps).

Por último, este proyecto busca que en los contratos que suscriban los establecimientos de crédito con establecimientos de comercio y administradores de pasarelas de pago se consignen, como mínimo, las siguientes obligaciones a cargo de éstos últimos:

Contar con certificación PCI.DSS versión 3.0 o posterior
Contar con política de tratamiento de datos personales
Adoptar mecanismos de autenticación del consumidor financiero
Contar con una política de administración del riesgo de lavado de activos y financiación del terrorismo
Adelantar campañas informativas sobre medidas de seguridad en operaciones
Informar al consumidor financiero sobre el procedimiento de pago, previo a su realización

---

# Información no financiera y RSC

Tras sólo un año de debate, se ha aprobado la Directiva europea de divulgación de información no financiera (2014/94/UE), que establece el marco en el que los Estados de la UE desarrollarán el modelo de información no financiera de las principales empresas de cada país. Se calcula que cerca de 6.000 compañías deberán hacer pública este tipo de información en los informes anuales correspondientes a 2016. La principal novedad es que estos requerimientos de información no se han incluido en una norma de responsabilidad corporativa, sino a través de la modificación de la cuarta y

la séptima directivas contables de la Unión Europea.

La Directiva afianza la tendencia de incluir dentro de la gestión ordinaria de las empresas los principales estándares de Responsabilidad Social, buscando acomodo en el informe anual de gestión. Afectará, por tanto, a todas las empresas que tengan más de 500 trabajadores, no aplicando a las subsidiarias que consolidan con otras sociedades.

Igualmente establece que las compañías deberán informar sobre cuestiones relativas al impacto medioambiental de su actividad, los efectos sobre la salud y seguridad, los gases de efecto invernadero, el uso de energía renovable, agua y contaminación atmosférica, las políticas sociales y con los empleados, la igualdad de oportunidades, las condiciones laborales, el respeto a los derechos sindicales, la salud y la seguridad, el diálogo con las comunidades locales, y las acciones para asegurar la protección y el desarrollo de dichas comunidades. Menciona también algún aspecto más general, como la protección de los Derechos Humanos y las medidas de prevención de abusos; temas ya definidos en regulaciones específicas, para la relación con empleados, clientes, proveedores, etc.

Las empresas deberán explicitar igualmente las medidas adoptadas para luchar contra la corrupción y el cohecho, así como los instrumentos que se apliquen para prevenir malas prácticas.

Para cada uno de los puntos anteriores, la información deberá incluir una breve descripción de su modelo de negocio; las políticas que se aplican y el debido control de las mismas; los resultados obtenidos; los riesgos ligados a las operaciones propias, con terceros, a productos o a servicios de la compañía, que puedan provocar impactos sobre alguno de estos asuntos; y la manera en la que los está gestionando la compañía; así como los indicadores no financieros específicos del sector.

La Directiva no especifica ningún formato de reporte, pero se refiere a marcos nacionales o internacionales de información financiera. La única condición es que la empresa deberá indicar cuál está utilizando. La Comisión Europea ha anunciado la publicación de una guía, que no será de obligado cumplimiento, sobre cómo elaborar esta información, con unos indicadores clave que faciliten la divulgación “pertinente, útil y comparable” de los resultados no financieros de las empresas.

Otro aspecto que ha propiciado la modificación de las directivas contables es el compromiso de la UE de promover la diversidad de género en las empresas europeas. Así, en un punto específico, la Directiva indica que las sociedades cotizadas deberán informar sobre la política, los objetivos y los resultados que aplican en materia de diversidad, en relación con los órganos de gobierno, dirección y supervisión, con indicadores como la edad, el sexo, la procedencia geográfica, la formación y la experiencia profesional.

Bajo el principio de cumplir o explicar, tan utilizado por los códigos de Gobierno Corporativo, si la compañía no puede revelar determinada información deberá explicar los motivos basándose en un posible impacto adverso para la compañía. Para la información sobre políticas de diversidad, las empresas cotizadas que carezcan de dichas políticas, podrán justificarlo acogiéndose al referido principio. Este aspecto ha flexibilizado la transposición de la norma por parte de los Estados miembros de la UE.

Cuando entre en vigor a nivel nacional, el auditor externo deberá comprobar que la información está incluida en el informe de gestión. Los Estados miembros, durante el proceso de trasposición de la directiva, podrán establecer el grado de revisión externa que deberá tener esta información.

La nueva Directiva afianza el valor de la información extrafinanciera, de los intangibles, del valor de la marca y de la reputación. Todo ello representa una ventaja competitiva excepcional para las empresas que quieran liderar el futuro.

# Instrucciones con respecto al Registro de Bases de Datos

El gobierno de Colombia a través de la Superintendencia de Industria y Comercio, presenta a los responsables de tratamiento de datos personales de acuerdo con la Ley 1581 de 2012 (Ley Habeas Data), los pasos a seguir para el registro de las bases de datos reguladas por dicha norma. Dentro de lo ítems objeto de registro se cuenta, el tipo de información almacenada, medidas de seguridad sobre la misma, procedencia u origen de los datos personales, si la información ha sido objeto transferencia, transmisión o cesión internacional, y reportes de novedades (quejas, incidentes de seguridad, etc.).

Adicionalmente se define el procedimiento y fechas para el registro de las bases de datos con base en el número de identificación tributaria (NIT) de cada empresa responsable del tratamiento de datos personales. Toda la información registrada deberá actualizarse en el primer trimestre de cada año, a partir del 2018.

Estos postulados, contenidos en la Circular 002 de 2015 de la Superintendencia de Industria y Comercio, buscan dar seguridad a los ciudadanos con respecto al tratamiento de sus datos personales, realizado por empresas del sector público y privado, evitando así la divulgación de los mismos de forma indiscriminada en el mercado.