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.

Ciberseguridad y nuevas tecnologías

A comienzos de abril fue publicada en Chile la nueva Ley Marco sobre Ciberseguridad para establecer los lineamientos, principios y normas para estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y de los particulares que prestan servicios financieros esenciales para el funcionamiento del país.

La ley introduce varios principios comunes a dichas entidades: control de daños, coordinación con la autoridad, respuesta responsable, seguridad informática, racionalidad y seguridad y privacidad desde el diseño y por defecto.

Igualmente, define los “servicios esenciales” como aquellos que son provistos por los organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional, los prestados bajo concesión de servicio público y por aquellas instituciones privadas que realicen las siguientes actividades: generación, transmisión o distribución eléctrica, transporte, almacenamiento o distribución de combustibles; suministro de agua potable o saneamiento; telecomunicaciones; infraestructura digital; servicios digitales y servicios de tecnología de la información gestionados por terceros; transporte terrestre, aéreo, ferroviario o marítimo, así como la operación de su infraestructura respectiva; banca, servicios financieros y medios de pago; administración de prestaciones de seguridad social; servicios

postales y de mensajería; y prestación institucional de salud por entidades tales como hospitales y clínicas.

La consideración de prestador de servicios esenciales lleva aparejados los deberes de: adoptar medidas permanentes para prevenir, reportar y resolver incidentes de ciberseguridad y reportar a la autoridad competente los ciberataques e incidentes de ciberseguridad acontecidos. También se introducen deberes específicos para las entidades consideradas «Operadores de Importancia Vital».

Por otro lado, a comienzos de mayo fue publicado en Perú el proyecto de Reglamento de la Ley que promueve el uso de la inteligencia artificial que completa las disposiciones contenidas en la Ley 31.814, publicada en julio de 2023, que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país, con la finalidad de fomentar la transformación digital, en un entorno seguro que garantice su uso ético, sostenible, transparente, replicable y responsable.

Entre otras cuestiones, atribuye a la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, la dirección, evaluación y supervisión del uso y la promoción del desarrollo de la inteligencia artificial y las tecnologías emergentes; contempla instrumentos para el uso y desarrollo de la inteligencia artificial; incorpora medidas para fortalecer el uso responsable y ético de la inteligencia artificial, de manera que el implementador de un sistema deba cumplir con ciertas condiciones de privacidad y transparencia, así como de seguridad y confianza en el uso y desarrollo de esta tecnología; o recoge que la clasificación de los sistemas basados en inteligencia artificial se haga en función del riesgo de afectación al trato equitativo, transparencia y derechos fundamentales generados por su uso.

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.

Gestión del riesgo de ciberseguridad y seguridad de la información

Con el fin de continuar promoviendo la adopción de mejores prácticas en materia de gestión del riesgo de ciberseguridad y seguridad de la información de las entidades financieras y con el propósito de estandarizar el reporte de métricas e incidentes relacionados con estos 2 riesgos, la Superintendencia Financiera de Colombia impartió instrucciones relacionadas con la Taxonomía Única de Incidentes Cibernéticos (por sus siglas TUIC), y el protocolo que deben utilizar las entidades en el reporte de, todas las comunicaciones, reportes de incidentes, alertas tempranas y boletines informativos relacionados con ello.

Otra de las novedades importantes de esta Circular, es la creación de Formato 408 “Reporte de métricas de Seguridad de la información y Ciberseguridad”, cuya periodicidad debe realizarse de forma trimestral. Las entidades financieras obligadas a realizarlo, debían presentar pruebas entre 18 y 22 de enero de 2021, con la información con corte al 31 de diciembre de 2020.

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.

Lineamientos y buenas prácticas para la gestión de la ciberseguridad

El pasado 31 de agosto la Superintendencia de Bancos e Instituciones Financieras de Chile publicó la circular Nº 3.640 que modifica el Capítulo 1-13 de la RAN relativo a la clasificación de gestión y solvencia con el fin de establecer los lineamientos y buenas prácticas para la gestión de la ciberseguridad, y el Capítulo 20-8 relativo a la Información de incidentes operacionales precisando aquéllos que deben ser comunicados al órgano regulador.

Capítulo 1-13. Clasificación de gestión y solvencia.

Tal y como define el nuevo Anexo que se introduce con motivo de la modificación, la ciberseguridad ha de entenderse como el *conjunto de acciones para la protección de la información presente en el ciberespacio*, así como de la infraestructura que la soporta, que tiene por objeto evitar o mitigar los efectos adversos de sus riesgos y amenazas inherentes, sobre la seguridad de la información y la continuidad del negocio de la institución*.

Los aspectos más relevantes que incluye la Circular son los siguientes:

Evaluación de la gestión de los Bancos: administración del riesgo operacional.

La norma señala la importancia de contar con una definición e identificación de los principales activos de información así como de la infraestructura física que soporta y resguarda la seguridad de los mismos. A estos efectos, se exige expresamente la gestión de la seguridad de los activos de información expuestos a riesgos en el ciberespacio.

Buena gestión.

Es necesario la disposición de estructuras dedicadas a la gestión de la ciberseguridad que contemplen los aspectos descritos en el nuevo Anexo 3 de la Circular en el que se regula en primer lugar, la gestión de la infraestructura crítica de ciberseguridad, y en segundo, la base de los incidentes de la misma.

Gestión de la infraestructura crítica de ciberseguridad.

El Directorio debe establecer un marco de gestión que contemple la estrategia de administración específica de este riesgo, el nivel de tolerancia, las responsabilidades de los participantes y las metodologías a utilizar para su gestión teniendo en cuenta las mejores prácticas y características de su actividad de negocio.

Base de incidentes de ciberseguridad.

En este sentido, se incluyen unas condiciones mínimas para el desarrollo y mantenimiento de una Base de Incidentes entre las que destaca la periódica toma de conocimiento de este tipo de incidentes por parte del Directorio y el consiguiente pronunciamiento sobre los mismos. Asimismo contempla las variables mínimas a considerar para la elaboración de esta base.

Capítulo 20-8. Información de incidentes operacionales

La norma también introduce modificaciones al Capítulo 20-8 motivadas por los nuevos riesgos operacionales que conlleva la evolución de la industria financiera, particularmente la incorporación de la tecnología en la forma de generar, procesar y administrar sus activos de información. Los aspectos más significativos que establece son:

Requisitos relativos a la información que se debe enviar a la SBIF cuando ocurran incidentes operacionales
Obligación de mantener adecuadamente informados a los clientes en determinados eventos
Deber de los bancos de compartir información de ataques relacionados a Ciberseguridad.

* Entorno que permite la interacción lógica, es decir no física, mediante la conexión de redes tecnológicas

---

Instrucciones para entidades vigiladas sobre ciberseguridad

La Circular Externa sobre medidas mínimas para la administración del riesgo de ciberseguridad complementa las medidas sobre administración de riesgo operativo y de seguridad de la información, para la administración de los riesgos de las entidades vigiladas por la Superintendencia Financiera de Colombia.

Dentro de los aspectos más relevantes se encuentran los siguientes:

Se establece la definición de Seguridad de la Información, Ciberseguridad, Ciberespacio, Ciberamenaza o amenaza cibernética, Ciberataque o ataque cibernético, Ciberiesgo o riesgo cibernético, Evento de ciberseguridad, *Security Information and Event Management (SIEM), Security Operation Center (SOC),* Vulnerabilidad, entre otros.
Obligación para las Entidades de contar con políticas, procedimientos y recursos técnicos y humanos necesarios para gestionar efectivamente el riesgo de ciberseguridad.
Adopción, por parte de las entidades vigiladas, de medidas mínimas sobre ciberseguridad como:
Políticas y procedimientos
Unidad especializada que gestione los riesgos
Sistema de Gestión para el riesgo de ciberseguridad
Empleo de mecanismos fuertes de autenticación
Establecimiento de estrategias de comunicación sobre ciberseguridad y reportes oportunos a autoridades y clientes
Evaluaciones periódicas sobre gestión de ciberseguridad y establecimiento de indicadores que midan la eficiencia y eficacia de la gestión de seguridad dela información y ciberseguridad
Etapas mínimas de gestión del riesgo de ciberseguridad (Prevención, Protección y Detección, Respuesta y Comunicación, y Recuperación y Aprendizaje).