FORO
JURÍDICO

La gestión de la Seguridad de la Información en el régimen peruano de Protección de Datos Personales

"Un sistema de información es un conjunto de elementos que capturan, almacenan, procesan y distribuyen información para apoyar la toma de decisiones, el control, análisis y visión en una organización; su seguridad debe evitar accesos no autorizados, adulteración, robo o daños físicos mediante políticas, procedimientos y técnicas para la salvaguarda del *hardware, software*, redes de telecomunicaciones y de datos".

Francisco Javier Alvarado*

Resumen: En el presente artículo se describe el régimen peruano de protección de datos personales con el foco en la normativa que obliga a los titulares o responsables de los bancos de datos a implementar las medidas de seguridad expuestas en el reglamento y en la directiva elaborada por la autoridad nacional. Pretende contribuir al conocimiento del alcance de dichas medidas en la actividad de las personas y organizaciones cuya gestión económica o social compromete la seguridad de datos personales, tomando en cuenta que son sujetos de fiscalización.

Palabras clave: Protección de datos personales; autodeterminación informativa; Seguridad de la Información; Ley de Protección de Datos Personales; La Autoridad Nacional de Protección de Datos Personales.

Abstract: This paper describes the peruvian legal system of personal data protection, paying special attention on a legislation that requires the owners or managers of data banks to implement security measures set out in the regulation drawn by the national authority. The analysis educates about the effects of this measures on individuals and organizations whose economic or social management compromises the security of personal data, taking into account that those are subject of control.

Keywords: Personal data protection; informational self-determination; information security; Peruvian Law of Personal Data Protection; The National Authority of Personal Data Protection.

(*) Abogado por la Pontificia Universidad Católica del Perú. Fedatario juramentado con especialización en Informática certificado por el Colegio de Abogados de Lima. Administrador de redes certificado con experiencia en gestión de bancos de datos y soporte a usuarios.

Introducción

Cumplido el plazo para la entrada en vigencia del régimen de protección de datos personales en el Perú, sustentado principalmente en la Ley de Protección de Datos Personales (en adelante, LPDP[1]) y su reglamento, es importante estudiar los alcances de las normas que obligan a los usuarios de los datos personales a protegerlos. En ese sentido, partimos de reconocer en la LPDP la obligación de cumplir con al menos tres obligaciones: el registro público de la titularidad del banco de datos personales; la atención a las solicitudes de las personas titulares de los datos; y la implementación de medidas de seguridad sobre los mismos, siendo esta última la que será materia de análisis en el presente artículo, motivado especialmente por lo novedosa que resulta esta materia para el análisis jurídico.

La información es entendida como un bien de utilidad social y, económicamente, se valora como tal; sin embargo, no fue hasta el desarrollo de la sociedad contemporánea que se le consideró como un bien jurídico y, en consecuencia, objeto de protección. El tratamiento automatizado de datos, al conservar, ceder, hacer inaccesible o propagar la información en forma instantánea e ilimitada en el espacio, suscitó como contraparte el aumento de los riesgos sobre su seguridad. La gestión de la seguridad de la información se despliega mediante un conjunto de políticas, prácticas, procedimientos, estructuras organizativas y funciones de *software* dirigidas a preservar su confidencialidad, integridad y disponibilidad.

Las organizaciones actuales dependen en mayor medida de la información, de las tecnologías que la procesan y transmiten, y de los sistemas de información, siendo estos últimos en los que se apoya su gestión. Los sistemas de información están formados por un conjunto de elementos –personal, datos, programas y equipos– que permiten el almacenamiento, procesamiento y transmisión de información con el objetivo de realizar tareas determinadas. Para la protección de dichos sistemas, existen cuatro tipos de medidas de seguridad: lógicas, físicas, administrativas y legales[2]. De esta manera, debido a la importancia de la información, se crea la necesidad de conocer el ordenamiento jurídico para definir las amenazas contra las que se protege el sistema, y las normas administrativas que determinen las responsabilidades correspondientes.

Previa a la implementación de dichas medidas, las organizaciones tienen el deber de identificar sus activos de información y su valor e importancia relativos; su inventario permite una protección eficaz, estableciendo el nivel de protección relativo al valor e importancia determinados. Son ejemplo de activos de información: los archivos y bancos de datos, la documentación del sistema, los manuales de los usuarios, el material de capacitación, los

(1) Ley N° 29733.
(2) LPDP, Artículo 16°.

procedimientos operativos o de soporte técnico, los planes de continuidad del negocio, la configuración del soporte de recuperación, la información archivada, el *software* de aplicación, el *software* del sistema y las herramientas y programas de desarrollo.

La protección de datos personales trae a colación la relación entre los conceptos "información" y "dato". El dato es un elemento del conocimiento que carece de significado fuera de su contexto pero que, complementado con otro u otros, mediante un proceso, brinda información a alguien en un momento y lugar determinados(3). Para el régimen peruano de protección de datos personales, éstos son toda información numérica, alfabética, gráfica, fotográfica o acústica que identifica o hace identificables a personas naturales, sus hábitos o cualquier tipo de información concerniente a su intimidad, a través de medios razonablemente utilizados(4). Los datos tienen el carácter de personales cuando alguien es capaz de vincular su información con una persona natural, aun si quien los posee no esté apto para realizar dicho enlace.

La complementación de datos se da con el acopio de aquellos datos referidos a una determinada materia que pueden ser utilizados por diversos usuarios; lo que se define como **banco de datos**. Los bancos de datos sujetos al régimen de la LPDP son aquellos conjuntos organizados de datos personales, automatizados o no, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso(5). Quienes son titulares de los bancos de datos personales son las personas que determinan la finalidad y el contenido de los mismos, el tratamiento a darles y las medidas de seguridad a implementar. Constituye tratamiento cualquier operación o procedimiento técnico, automatizado o no, que permita alguna forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

1. Cumplimiento del principio de seguridad en el tratamiento de datos personales

La seguridad de la información es uno de los **principios rectores** establecidos en la LPDP y, como tal, es una obligación de los titulares y encargados de los bancos de datos personales y, en general, de todos los que tomen parte en relación con el tratamiento de datos personales. El dictamen del proyecto de la LPDP describe dichos principios como:

> normas que tienen la estructura de mandatos de optimización [que] no determinan exactamente lo que debe hacerse, sino que ordenan que algo sea realizado en la mayor medida posible, dentro de las posibilidades jurídicas y reales existentes (..). orientan y determinan el comportamiento de todos los que van a participar en el tratamiento de datos personales, señalando las reglas de conducta que ellos deben observar.

Sin embargo, es importante entender que la aplicación de estos principios no se reduce a proponer una serie de ideas fundamentales que orienten las conductas de los responsables, sino que su incumplimiento constituye una infracción, cuya consecuencia será la imposición de multas y otro tipo de sanciones.

En atención al principio de seguridad, el titular del banco de datos personales debe hacer propias las

(3) DE PABLOS, C., LÓPEZ, J., MARTÍN, S., MEDINA, S., MONTERO, A., NÁJERA, J. *Dirección y gestión de los sistemas de información en la empresa: una visión integradora*. Madrid, España: ESIC. 27, 2006. Consulta: 15 de diciembre 2015. <https://books.google.com.pe/books?id=OqlSVYn0fl0C&lpg=PP1&pg=PP1#v=onepage&q&f=true>.

(4) Reglamento de la LPDP, Artículo 2°.

(5) LPDP, Artículo 2°.

medidas técnicas, organizativas y legales necesarias para garantizar confidencialidad, integridad y disponibilidad de los mismos, con el fin de evitar su adulteración, pérdida, desviación de información, intencionada o no, y cualquier tratamiento ilegal; sin perjuicio de que estos riesgos provengan de la acción humana o del medio técnico utilizado. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.

El principio de seguridad, a diferencia de los demás principios rectores que específicamente obligan al cumplimiento de normas o criterios en el tratamiento de datos personales, exige una actitud más activa por parte del responsable, que evalúe e implante las medidas necesarias para gestionar la seguridad de la información tratada. Por tanto, "el cumplimiento del principio de seguridad constituye la principal fuente de obligaciones y porqué [sic] no decir, también de costes que debe afrontar el responsable"[(6)].

De esta manera, se puede afirmar que los objetivos del principio de seguridad son:

- Facilitar la implantación de una gestión en continua evaluación que, mediante la categorización de los bancos de datos personales en razón a los riesgos que conlleva su sensibilidad y el tratamiento dado, complemente las medidas técnicas;
- Informar a los usuarios para que tomen conciencia de la protección requerida; y
- Exigir un nivel de seguridad equilibrado entre los riesgos, las técnicas de seguridad y el costo de las medidas.

En ese sentido, la LPDP establece como mandato la prohibición del tratamiento de datos personales en bancos de datos que no cumplan los requisitos y las condiciones de seguridad establecidos por la Autoridad Nacional de Protección de Datos Personales y en disposiciones especiales contenidas en otras leyes; por ejemplo, las del sector de comunicaciones y telecomunicaciones, siempre que no se opongan a lo establecido en la misma LPDP y su reglamento. Consecuentemente, la mencionada ley otorga a dicha autoridad nacional la función de emitir directivas, especialmente en materia de seguridad de los bancos de datos personales, así como supervisar su cumplimiento en coordinación con los sectores involucrados. La Autoridad Nacional de Protección de Datos Personales la ejerce la Dirección General de Protección de Datos Personales (DGPDP) del Ministerio de Justicia y Derechos Humanos.

Las disposiciones relativas a las medidas de seguridad son de obligatorio cumplimiento por el titular o encargado del banco de datos personales o el responsable o encargado del tratamiento, siempre que se encuentre establecido en territorio peruano. Como ya se expusiera anteriormente, el **titular del banco de datos personales** es quien determina su finalidad y contenido, el tratamiento y las medidas de seguridad; siendo **encargado del banco de datos personales** quien, solo o actuando conjuntamente con otro, realiza el tratamiento de los datos por encargo del titular del banco de datos personales.

La naturaleza jurídica del **tratamiento de datos personales** se define en el artículo 2° de la LPDP como:

> cualquier operación o procedimiento técnico que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo,

(6) ZABALLOS PULIDO, E. *La protección de datos personales en España: evolución normativa y criterios de aplicación*. Universidad Complutense de Madrid. Facultad de Derecho, 222, 2013. Consulta: 15 de diciembre 2015: <eprints.ucm.es/22849/1/T34733.pdf>.

> supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

Al respecto, es **responsable** del tratamiento quien decide sobre el mismo, aún cuando los datos no formen parte de un banco, y es el **encargado** del tratamiento quien lo realiza, pudiendo ser el propio titular del banco de datos personales el encargado del mismo u otra persona por encargo del titular, en virtud de una relación jurídica que les vincule y delimite el ámbito de su actuación; incluyendo a quien lo realice por orden del responsable del tratamiento, cuando éste se realice sin la existencia de un banco de datos personales.

La siguiente tabla expone los sujetos y tipos legales descritos:

Banco de datos personales	Tratamiento de datos personales
Titular	Responsable
Encargado	Encargado

El reglamento de la LPDP trata de manera separada las medidas de seguridad aplicables al tratamiento de datos digitalizados de las aplicables a la documentación no automatizada.

1.1 Seguridad para el tratamiento de la información digital

Así, para el caso de los sistemas informáticos que manejen bancos de datos personales, éstos deberán incluir en su procesamiento medios para el registro e identificación de usuarios (por ejemplo, usuario-contraseña, certificados digitales, *tokens*, etcétera), la gestión y verificación periódica de los privilegios asignados a los mismos y el control de acceso a los datos personales, los que estarán definidos en un procedimiento documentado. De igual manera, deberán generar y mantener registros legibles y oportunos que evidencien las interacciones con los datos para fines de trazabilidad, lo que incluye información de las cuentas de usuario como, por ejemplo, las horas de inicio y cierre de sesión y las acciones relevantes.

También deberán implementarse medidas de seguridad en los ambientes en los que se procese, almacene o transmita la información, tomando como referencia las recomendaciones de seguridad física y ambiental recogidas en la Norma Técnica Peruana ISO/IEC 17799 EDI titulada "Código de buenas prácticas para la gestión de la seguridad de la información".

Además, ante una interrupción o daño del sistema informático, se deberá considerar la conservación de la información poniendo en funcionamiento un procedimiento de copia de respaldo del banco de datos personales con la verificación de su integridad y la recuperación que garantice el retorno al estado en el que se encontraba al momento en que se produjo.

Por último, en caso de transferencia lógica o electrónica de los datos personales, se deberán tomar medidas de seguridad para evitar el acceso no autorizado, la pérdida o corrupción durante el tránsito desde los ambientes de procesamiento o almacenamiento hacia cualquier destino fuera de las instalaciones físicas del encargado del tratamiento. Ejemplo de dichas medidas son el cifrado de datos, el uso de firmas digitales o de las sumas de verificación.

1.2 Almacenamiento de documentación no automatizada

Para el tratamiento de documentos no automatizados con datos personales, deberán tomarse medidas para su almacenamiento en armarios, archivadores u otros elementos ubicados en ambientes protegidos con mecanismos de cerradura u otro dispositivo

equivalente en las puertas. Éstos deberán permitir mantener el control de acceso a los mismos, o las medidas alternativas que las directivas de seguridad de la DGPDP establezcan en caso que, por las características del local disponible, no fuera posible cumplir lo anteriormente establecido.

También se deberán implementar mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios, con el fin de limitarlos exclusivamente al personal autorizado. El acceso de personas no incluidas entre las autorizadas deberá registrarse de acuerdo a las directivas de seguridad que emita la DGPDP.

Se deberán implantar medidas de seguridad para que la generación de copias o la reproducción de los documentos puedan ser realizadas únicamente bajo el control del personal autorizado. Además, se debe incorporar los recaudos necesarios para que se destruyan las desechadas, de manera que no se permita acceder posteriormente a la información o la recuperación de las mismas. En caso de traslado de documentación no automatizada, contenida en un banco de datos personales, se deberán adoptar medidas que impidan el acceso o manipulación de la información.

En cualquier caso, para la realización de servicios prestados que no impliquen el tratamiento de datos personales como, por ejemplo, el mantenimiento de equipos o de *software*, se deberán aplicar medidas para limitar el acceso a los datos personales al personal que realiza estos servicios, a los soportes que los contengan o a los recursos del sistema de información. Cuando el personal contratado para esas prestaciones sea ajeno a la entidad titular o responsable de los datos, se deberá establecer expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los que hubiesen podido conocer con motivo del servicio prestado.

Por último, los titulares de los bancos de datos personales deberán describir técnicamente las medidas de seguridad a ser aplicadas en la solicitud para su inscripción en el Registro Nacional de Protección de Datos Personales a cargo de la DGPDP.

2. Autorregulación y protección de derechos constitucionales

En este punto, es necesario tratar el fin último de la protección de datos personales, esto es, el derecho fundamental a la intimidad. Cada vez con mayor fuerza, el poder se apoya en medios que facilitan el atisbo de las personas, sus conductas, hábitos y preferencias. La utilización de dichos medios por sujetos privados crea, por ejemplo, condiciones para que los ciudadanos se encuentren en desventaja frente a empresas que convierten su información personal en una mercancía.

La capacidad de recolectar información, esencial para ejercer esa vigilancia, permite mejorar la calidad de los servicios, vender más bienes y, en general, brindar condiciones de vida más favorables. Por otro lado, empresas globales cuentan con información agregada de la que hasta los mismos Estados carecen. En esta situación, es esencial que el Derecho garantice que el afán comercial no predomine sobre el interés social; por ello, el desafío que se le plantea consiste en evitar generar una situación de supervisión de las personas, las cuales son carentes de protección a su intimidad.

La intimidad, como un espacio personal ajeno a la injerencia de la sociedad o el Estado, configura un límite al poder social y político: el respeto que merece constituye una prueba de la libertad como realización plena del individuo. La noción de intimidad que la

filosofía clásica asemeja a la soledad y al aislamiento del individuo se descarta en el campo jurídico; el problema de la intimidad se presenta jurídicamente sólo a través de las manifestaciones o incidencias externas de la vida privada y cuyo ejercicio se halla garantizado. La convivencia, cuya base es la comunicación, socializa lo íntimo del individuo y origina la propia noción de intimidad como una categoría cultural e histórica. De esta manera, el derecho a la intimidad supone la voluntad de su titular de mantener lo que él considere bajo la condición de íntimo o privado, y consiste en controlar esa zona de retiro y secreto que voluntariamente ha sido dispuesta por el individuo. Esta capacidad de control es considerado un derecho de autodeterminación.

La sociedad resulta el sujeto pasivo del derecho a la intimidad, en tanto que todas las personas están obligadas a respetarlo; sin embargo, ésta se individualiza en la situación o hecho de recolectar datos o información, obligando al responsable a que éstos sean lo estrictamente relevantes para los fines solicitados, a conservarlos solo por el tiempo necesario y a no utilizarlos ni comunicarlos con propósitos que no sean los debidamente autorizados. De lo anterior se desprende la importancia de gestionar la seguridad de la información en busca de establecer políticas, programas y controles para mantener la confidencialidad, integridad y disponibilidad de la misma. Para este fin, se debe tener en cuenta que la seguridad no se obtiene sino como resultado de un proceso continuo que va reconociendo las vulnerabilidades y amenazas, sus causas, la probabilidad de que ocurran y el daño que ocasionarían. Conocidas éstas, deberán tomarse las medidas de seguridad correspondientes.

En resumen, el concepto de seguridad de la información se puede definir como el conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información.

Un sistema de información es un conjunto de elementos que capturan, almacenan, procesan y distribuyen información para apoyar la toma de decisiones, el control, análisis y visión en una organización; su seguridad debe evitar accesos no autorizados, adulteración, robo o daños físicos mediante políticas, procedimientos y técnicas para la salvaguarda del *hardware, software,* redes de telecomunicaciones y de datos.

Desde el siglo pasado, el Instituto Británico de Normas Técnicas (BSI[7] por sus siglas en inglés) y la Organización Internacional de Normas Técnicas (ISO[8] por sus siglas en inglés) han elaborado parámetros para las técnicas de operación, fabricación y desempeño: en 1995, el BSI publicó la primera norma técnica de seguridad, codificada como BS7799, con el fin de asegurar el naciente comercio electrónico. En diciembre del año 2000, la ISO publica una revisión de la norma británica bajo el nombre de ISO17799, la que, desde su publicación y la de sus sucesivas revisiones y su reconversión en la serie 27000 fue y es reconocida mundialmente como la norma técnica de las mejores prácticas de seguridad de la información. De ahí la utilidad de tratar el concepto de **normalización** como el proceso de elaborar, aplicar y mejorar normas con el fin de obtener un resultado ordenado en actividades científicas, industriales o económicas para el beneficio y con la cooperación de todos los involucrados.

Sobre este punto, cabe precisar que las normas técnicas son un conjunto de especificaciones obtenidas como resultado de la cooperación de la

(7) *British Standard Institute*.
(8) *International Organization for Standardization*.

ciencia, la tecnología y la experiencia, aprobadas mediante el consenso de todos los sujetos interesados que participan de un organismo de normalización y, como tales, son el resultado de la autorregulación. Además, se caracterizan por su publicidad y su vinculación con el cumplimiento de objetivos generales dirigidos a obtener beneficios sociales. Aunque comúnmente están referidas a un producto o una tecnología en particular, a semejanza de las normas jurídicas, pretenden la seguridad y la generalidad.

El conocimiento que poseen quienes desarrollan y aplican las innovaciones tecnológicas es ajeno tanto al legislador como a la Administración Pública, quienes enfrentan su creciente incapacidad para regularlas y controlar sus riesgos. Además, la mayor complejidad de las funciones que el Estado asume y sus limitados recursos para preparar a la burocracia ante ese reto le impele a requerir la colaboración de los expertos privados, cuyo conocimiento técnico evoluciona en mayor medida. Dadas esas condiciones, el propósito regulador sobre la complejidad tecnológica sólo resulta posible a partir de la autorregulación.

Es así como la capacidad de autorregularse resulta una fórmula con la que los Estados cuentan cada vez más para enfrentar su dificultad en proteger la dignidad de las personas en una sociedad en la que la ciencia y la técnica dominan los procesos que generan amenazas en contra de ese bien jurídico. Asimismo, permite establecer una correspondencia entre los responsables de las amenazas y las medidas que garantizan su protección. Por el hecho de configurar espacios complejos que resultan impenetrables para los poderes públicos, la incesante y extensiva aplicación de la tecnología de la información se desenvuelve en gran medida al margen de su regulación e intervención, lo que desafía al Derecho a renovar muchos de sus objetivos e instrumentos con el fin de controlar y racionalizar estas nuevas fuerzas que actúan en la sociedad.

El término "regulación" implica heteronomía, esto es, que la voluntad del sujeto regulado se rija por imperativos de la autoridad reguladora. La regulación, por tanto, es el instrumento o conjunto de instrumentos por los que se somete la acción de un sujeto a una regla determinada, éste es el sentido que se le reconoce en el ámbito del Derecho, por lo que se le identifica con la elaboración de normas jurídicas[9]. Cuando los instrumentos de regulación ordenan la actividad del mercado se caracteriza una regulación económica, cuando tutelan los derechos constitucionalmente protegidos se caracteriza una regulación de policía[10], la que –mediante reglamentaciones técnicas– determina condiciones de seguridad para aquellos derechos estableciendo controles preventivos y sanciones en caso de incumplimiento.

Por otro lado, la capacidad de autorregularse está sujeta exclusivamente a la dinámica social o del mercado y, por tanto, se desarrolla sin control estatal; sin embargo, en la actualidad sus efectos alcanzan al Estado y marcan una nueva etapa en el desarrollo de sus relaciones con la sociedad. El interés actual en la autorregulación se debe a que sus efectos están excediendo del ámbito privado para convertirse en referencia inevitable en las consideraciones de los poderes públicos, haciendo evidentes las modificaciones en la correlación entre lo privado y lo público. Esta tendencia obliga al Estado a considerar las reglas, referencias y decisiones de

(9) ALVARADO, F. J. *El régimen jurídico del control sobre el uso de recursos informáticos ejercido por los empleadores en el Perú*. Pontificia Universidad Católica del Perú. Facultad de Derecho, 2006 p. 71.

(10) Íbid.

la autorregulación. Los fines de la regulación de policía se consideran hoy también como propios de la sociedad, por lo que a través de la regulación de la autorregulación se involucra a los sujetos privados en la protección de los derechos constitucionales.

Muchas de las reglas propias de grupos profesionales son documentadas actualmente en forma de códigos, normas técnicas o protocolos de actuación que hacen más fácil las relaciones entre el ámbito profesional y el jurídico. La aceptación consensual de las reglas autoimpuestas por aquellos le da el carácter vinculante y cuanto mejor organizado esté el grupo en el que se generan, más se aproximará ese consenso a un acuerdo jurídico. Estos instrumentos que ya funcionan en el Derecho privado se han ido extendiendo al Derecho público mediante la transcripción de las normas técnicas o la remisión legal o reglamentaria a éstas, estableciéndose así la conexión entre ambos.

Es de esa manera que la autorregulación, generada fuera del sistema legal, resulta jurídicamente relevante al volverse inteligible y aceptable por el Derecho. Así es como el Estado, en su función de garante de los bienes más preciados de la sociedad, fomenta, regula o impone el cumplimiento de normas técnicas que hacen posible la protección de tales bienes.

Precisamente, uno de los presupuestos para la autorregulación a través de normas técnicas se da en el ejercicio del poder que da el uso de la informática y las telecomunicaciones, especialmente por la amenaza a la intimidad que el procesamiento y transmisión de datos personales conlleva. Con el fin de prevenir el daño a derechos fundamentales protegidos constitucionalmente, el Estado utiliza las normas de la autorregulación como instrumentos al servicio del interés público, considerándolas como formas de regulación que resultan siendo una **autorregulación regulada** fomentada, dirigida e instrumentalizada por el mismo Estado.

De ello se infiere que el Estado utiliza la autorregulación como una forma de regulación indirecta: por medio de la autorregulación regulada, la Administración Pública supervisa los actos de aprobación y cumplimiento de normas y controles privados que garantizan la capacidad técnica y el sometimiento a fines públicos de los sujetos autorregulados con el objeto de minimizar los riesgos generados por aquellos. Debido a que la responsabilidad directa de la reducción de los riesgos corresponde a quienes los generan y los conocen, éstos se ven impelidos a documentar normas técnicas útiles para el desarrollo de controles internos, a contratar asesoría en la implementación de tales normas y controles y a auditar su gestión eficiente.

La existencia de normas técnicas para un determinado sector que el Estado pretende regular le permite incorporar tales normas en sus reglamentaciones, ya sea al transcribirlas o remitiéndose al texto de las mismas, de manera tal que se establece la obligatoriedad a las normas citadas (la llamada "remisión estática") o, inclusive, haciendo obligatorias las posteriores modificaciones a esas normas (la llamada "remisión dinámica"). La regulación de la autorregulación otorga un mayor grado de confianza en esta última, cuando su cumplimiento atribuye efectos probatorios en procedimientos administrativos para el otorgamiento, denegación o control de autorizaciones; efectos probatorios que a su vez adquieren especial significado cuando las normas jurídicas incorporan conceptos indeterminados como el de "buenas prácticas" o "la mejor tecnología disponible".

Por ello, se puede afirmar que todos los instrumentos de autorregulación producen efectos probatorios en la medida que proporcionan información útil, ya sean indicios, presunciones o dictámenes periciales anticipados relacionados con la certeza de hechos o el cumplimiento de normas. Así, en todo proceso en el que exista controversia sobre la diligencia

de un profesional u organización con relación a su responsabilidad en la ocasión de daños, los instrumentos de autorregulación documentan las reglas técnicas que rigen la actividad en cuestión. El cumplimiento de requisitos de seguridad establecidos en normas técnicas puede enervar una demanda por daños ocasionados; bastará para ello con verificar que los instrumentos de autorregulación sean los adecuados para la comprobación de la diligencia debida y que se ha cumplido con las reglas. Es a través de la remisión que los poderes públicos asumen los resultados de la autorregulación. La remisión se da a partir de una norma jurídica y tiene como destino un instrumento de autorregulación –que comúnmente se trata de normas técnicas– debidamente identificado.

De esa manera, se da una transformación de la autorregulación en norma jurídica. La incorporación de la norma técnica al ámbito público supone el abandono del marco del Derecho privado propio de la autorregulación y, por tanto, de su voluntariedad. Los efectos vinculantes de la técnica de la remisión han sido reconocidos explícitamente en el caso de las normas técnicas y se extienden también a los **códigos de buenas prácticas** en materia de seguridad. El concepto de "Buena Práctica" se aplica a las acciones de un profesional o una organización responsable en el ejercicio de su actividad, quienes implantan determinados controles de cumplimiento. La documentación de dichos controles constituye un instrumento de autorregulación que detalla cómo se aplican esas buenas prácticas.

En nuestro país, la aprobación de normas técnicas es competencia del recientemente creado Instituto Nacional de Calidad (INACAL), función que le ha sido transferida desde la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias del Instituto de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) que aprobó la norma técnica peruana (NTP) ISO/IEC 27001:2014, que expone los requisitos para implantar Sistemas de Gestión de Seguridad de la Información (SGSI). La Comisión de Reglamentos Técnicos y Comerciales, que antecedió a aquella en el mismo INDECOPI, aprobó, a su vez, la NTP-ISO/IEC 17799:2007 que contiene el Código de Buenas Prácticas para la gestión de la seguridad de la información. La elaboración de normas técnicas peruanas procede mediante la adopción de normas técnicas internacionales introduciendo en ellas condiciones particulares de aplicación en el país, de ahí la referencia en la nomenclatura.

Como ya se expresó anteriormente, la LPDP establece que los requisitos y condiciones que deben reunir los bancos de datos personales en materia de seguridad son los establecidos por la Autoridad Nacional de Protección de Datos Personales, esto es, la DGPDP, para lo cual ésta ejerce la función de emitir las directivas que correspondan a la mejor aplicación de la Ley y su reglamento en esta materia, y la de supervisar su cumplimiento. Mediante Disposición Complementaria, la propia LPDP mandó elaborar a dicha autoridad la directiva de seguridad de la información de los bancos de datos personales.

3. Directiva de Seguridad

La Directiva de Seguridad aprobada por la DGPDP, con el fin de garantizar el cumplimiento de las medidas de seguridad necesarias, expone un sistema de condiciones, requisitos y medidas de seguridad. En el mismo, se consideran como condiciones de seguridad aquellas recomendaciones para la implementación de requisitos de seguridad que, a su vez, sirven como elementos de prueba del cumplimiento de las mencionadas condiciones; mientras que las medidas de seguridad son las prevenciones conducentes al cumplimiento de dichos requisitos.

3.1 Condiciones de seguridad

Las condiciones de seguridad suponen el compromiso por parte del titular del banco de datos de disponer de los recursos necesarios para:

- Proteger los datos personales;
- Comprender el contexto organizativo, tecnológico, jurídico, legal, contractual, reglamentario y físico para el tratamiento y protección de esos datos;
- Determinar y autorizar roles y responsabilidades para cumplir con la política de seguridad; y
- Desarrollar un enfoque de gestión del riesgo.

Para determinar los requisitos y medidas a implementar, la propia directiva establece una categorización para el tratamiento de los datos en relación con el volumen de registros que contiene el banco; el número de datos personales por cada titular; el período de tiempo establecido para cumplir con la finalidad del tratamiento; la calidad personal del titular del banco de datos; el acceso o tratamiento en uno o múltiples locales y el tratamiento de datos personales sensibles.

Las categorías de tratamiento se exponen en la tabla siguiente:

	Volumen de registros	Número de datos	Cumplimiento de la finalidad	Titularidad del banco de datos	Local	Datos sensibles
Básico	Hasta 50	Hasta 5	No aplica	Persona natural	Único	No
Simple	Hasta 100	Más de 5	Menos de 1 año	Persona natural o jurídica	Único	No
Intermedio	Hasta 1000	Más de 5	Más de 1 año	Persona natural o jurídica	Único	Sí
Complejo	Indeterminado	Más de 5	Más de 1 año	Persona jurídica o entidad pública	Múltiple	Sí
Crítico	Indeterminado	Más de 5	Más de 1 año	Persona jurídica o entidad pública	Múltiple	Sí

3.2 Requisitos de seguridad

En ingeniería de sistemas, un requisito es una necesidad documentada sobre el contenido, forma o funcionalidad de un servicio, tomando en cuenta las necesidades de las partes interesadas que pueden entrar en conflicto. En este sentido, los requisitos establecidos en la directiva de seguridad de la LPDP para todas las categorías de tratamiento de datos personales son:

- Declarar y comunicar formalmente una política de protección de datos personales que incluya compromisos de cumplimiento de los requisitos de seguridad, de respeto a los principios de la LPDP y de mejora continua.
- Documentar los procesos y procedimientos del tratamiento de datos personales que permitan el control de las decisiones sobre aquel, aún cuando aquél se realice por subcontrato.
- Implementar las medidas de seguridad que correspondan al nivel de protección de datos personales según la categoría correspondiente.

- Elaborar y mantener un documento maestro de seguridad de la información del banco de datos personales.
- Documentar el compromiso de confidencialidad del personal que interviene en los procesos y procedimientos para el tratamiento de datos personales.
- Implementar y documentar los siguientes procedimientos[11]:
  - En la categoría de tratamiento simple: para el control de documentos y registros, para el registro de personal con acceso autorizado, de incidentes y de medidas adoptadas;
  - Además, en las categorías de tratamiento intermedio y complejo: para el registro de accesos, de auditorías y problemas de seguridad; y
  - En caso de tratamiento crítico: para el registro de control de acceso y demás procedimientos incluidos en la normativa técnica del SGSI.
- Tomar decisiones bajo el enfoque de riesgos, contando con un correspondiente plan para el tratamiento de datos personales[12].
- Los establecidos solo para las categorías de tratamiento complejo y crítico.
- Incorporar los requisitos de seguridad para los bancos de datos personales en el alcance de SGSI, según la norma técnica vigente.

3.3 Medidas de seguridad

El titular del banco de datos personales debe designar a una persona natural como responsable de seguridad, otorgándole la capacidad y la autoridad para coordinar la aplicación de la directiva de seguridad de la LPDP.

De acuerdo a su naturaleza, las medidas de seguridad se agrupan en organizativas, jurídicas y técnicas.

Corresponde a las organizativas:

- Disponer una estructura de roles y responsabilidades para la protección de datos personales.
- Documentar su compromiso de respeto a los principios de la LPDP.
- Verificar de manera periódica y documentada la efectividad de las medidas de seguridad.

Aplicables a las categorías de tratamiento intermedio, complejo y crítico:

- Documentar los procedimientos para el tratamiento de datos personales.
- Desarrollar un programa de creación de conciencia y entrenamiento en materia de protección de datos personales.
- Desarrollar un procedimiento de auditoría anual respecto de las medidas de seguridad implementadas.
- Desarrollar un procedimiento de gestión de incidentes.
- Desarrollar un procedimiento de asignación de privilegios de acceso y su correspondiente registro.

Destinados a las categorías de tratamiento complejo y crítico:

- Registrar a los operadores del banco de datos personales y controlar su acceso con fines de trazabilidad.

(11) Opcional para la categoría de tratamiento básico.
(12) Opcional para las categorías de tratamiento básico y simple.

- Adecuar al régimen de protección de datos personales los sistemas de gestión o las aplicaciones existentes que toman parte en el tratamiento de datos personales y los procesos de negocio involucrados.

Corresponde a las jurídicas:

- Mantener formatos de consentimiento para el tratamiento de datos personales.

Para las categorías de tratamiento intermedio, complejo y crítico:

- Adecuar al documento de compromiso de confidencialidad establecido como requisito de los contratos del personal y de terceros relacionados con el tratamiento de datos personales.

Por último, a las medidas de seguridad técnicas. Estas están agrupadas con relación a la protección contra el acceso no autorizado al banco de datos personales, la alteración, la pérdida y el tratamiento no autorizado de datos personales.

Las relativas a la protección contra el acceso no autorizado son:

- Registrar a los usuarios con un identificador, al usuario que lo autoriza o da de baja y la fecha y hora de la anotación.

- Registrar las revisiones periódicas de los privilegios de acceso a los datos personales del personal autorizado, al menos semestralmente.

- Ubicar los bancos de datos no automatizados en ambientes aislados, protegidos por cerradura o mecanismo de protección similar contra acceso físico no autorizado a cargo del titular o del responsable que aquel designe.

Para el tratamiento de la información digital:

- Gestionar el uso de contraseñas mediante el control de la asignación y uso forzoso de contraseñas fuertes, solicitando a los usuarios mantener la confidencialidad de las mismas, permitiéndoles cambiarlas, almacenándolas de manera cifrada, en caso de contar con servidor de autenticación, y bloqueando el acceso fallido consecutivo.

- Asignar a cada usuario, como mínimo, un nombre/contraseña como identificador único de acceso para su autenticación.

Para las categorías de tratamiento intermedio, complejo y crítico:

- El identificador único de acceso del usuario deberá estar asociado a un perfil y a sus accesos autorizados y se deberán implementar mecanismos de restricción que eviten su acceso a recursos no autorizados. La autenticación puede darse por contraseña, dispositivo identificador *(token)*, dispositivo biométrico, firma digital, tarjetas de coordenadas o similares.

- Implementar un registro de accesos con, al menos, fecha y hora de la ocurrencia, el usuario, el identificador del titular del dato tratado y el motivo.

"En atención al principio de seguridad, el titular del banco de datos personales debe hacer propias las medidas técnicas, organizativas y legales necesarias para garantizar confidencialidad, integridad y disponibilidad de los mismos, con el fin de evitar su adulteración, pérdida, desviación de información, intencionada o no, y cualquier tratamiento ilegal; sin perjuicio de que estos riesgos provengan de la acción humana o del medio técnico utilizado. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate".

Contra la alteración no autorizada:

- Registrar a los usuarios con privilegios para el tratamiento de los datos personales.
- Designar al personal encargado, en caso de generar o eliminar copias o reproducciones de documentos con datos personales, de atender o supervisar los equipos autorizados para dichas operaciones, el retiro de los originales al culminar y el registro de las copias o reproducciones.
- Documentar cada autorización de retiro o traslado de datos personales fuera de los ambientes en donde se ubican.

En caso de traslado de datos personales en soporte físico:

- Utilizar recipientes con mecanismo de verificación de invulnerabilidad que eviten su acceso o legibilidad.

En caso de encontrarse en soporte informático:

- Utilizar escritura con clave secreta para cifrar los datos a trasladar y un mecanismo de verificación de integridad (suma de verificación MD5, firma digital o similar).
- Utilizar mecanismos de borrado total o destrucción del medio removible, de modo que no permitan la recuperación de los datos personales, a cargo de personal autorizado por el titular del banco.

Contra la pérdida de datos personales[13]:

- Realizar copias de respaldo de los datos personales, protegidas mediante técnicas de cifrado, y almacenarlas en local seguro y distante del ambiente de tratamiento para su recuperación en casos de pérdida o destrucción.
- Autorizar toda copia o recuperación de datos personales.
- Documentar la realización de pruebas de recuperación de las copias de seguridad.

Por último, las medidas contra el tratamiento no autorizado:

- Informar con detalle a la persona cuya información es tratada sobre incidentes de seguridad que afecten significativamente sus derechos morales o patrimoniales, tan pronto se confirme el hecho.
- Registrar los incidentes de seguridad que afecten la confidencialidad, integridad y disponibilidad de los datos personales o los incumplimientos de las medidas de seguridad para su información al titular o encargado del banco, quien deberá coordinar una respuesta rápida y efectiva.

Para las categorías de tratamiento simple, intermedio, complejo y crítico:

- Disponer el cifrado de todo dato o información personal que ha de ser transmitido electrónicamente o el uso de protocolos de comunicación cifrados y firmas digitales para validar la identidad del emisor.
- Restringir el uso de equipos de fotografía, registro audiovisual o similares en el área de tratamiento de datos personales.

Para las categorías de tratamiento intermedio, complejo y crítico:

- Disponer el mantenimiento preventivo y correctivo de los equipos utilizados para el tratamiento de datos personales y su protección contra *software* malicioso de manera de asegurar su disponibilidad y proteger la integridad de los datos.
- Determinar el empleo de mecanismos de control de acceso y cifrado para el almacenamiento de datos personales electrónicos.

(13) Medidas de seguridad técnica opcionales para las categorías de tratamiento básico y simple.

- Disponer auditorías[14] para verificar el cumplimiento de los requisitos de la directiva de seguridad del régimen de PDP e implementar las acciones correctivas consecuentes y la mejora continua.

De manera más específica, la Directiva establece una orientación para su cumplimiento en casos de las categorías de tratamiento complejo y crítico de bancos de datos personales, tanto para las entidades públicas del Sistema Nacional de Informática, obligadas a implementar sus propios sistemas de gestión de seguridad de la información normalizados por la NTP-ISO/IEC 27001, como para las personas jurídicas que lo implementen de manera voluntaria. Además de cumplir con la mayor parte de los requisitos y medidas de la directiva de seguridad, necesariamente deberán identificar cuáles son los aspectos de esta última que no estén contemplados en el SGSI, a fin de que estén debidamente atendidos. Igualmente, podrán utilizar las normas técnicas ISO 31000 o ISO/IEC 27005 como referencias para la gestión del riesgo.

4. Fiscalización

El cumplimiento en la implementación de las medidas de seguridad es fiscalizado por la Dirección de Supervisión y Control de la DGPDP. El procedimiento se puede iniciar de oficio o por denuncia de parte, en el cual se requerirá al titular o encargado del banco de datos personales, o a quien resulte responsable, la documentación o información relativa al tratamiento. El objeto del procedimiento de fiscalización es determinar la presunta comisión de infracciones previstas en la LPDP y su reglamento. Ésta terminará con un informe en el que se pronuncia sobre la existencia de elementos o la concurrencia de circunstancias que justifiquen o no la iniciación del procedimiento sancionador. En el procedimiento de fiscalización se podrán llevar a cabo visitas a los lugares en donde se encuentra la persona a quien se fiscalizará o donde se encuentren los bancos de datos personales objeto del procedimiento para obtener los elementos de convicción necesarios. En un acta se constatarán las actuaciones practicadas en presencia de la persona con quien se tratará durante la visita y también se anotará si ésta se niega a colaborar u observa una conducta obstructora; ello sin perjuicio de que aquella pueda, a su vez, formular observaciones al acto o manifestar lo que a su derecho convenga.

En el informe de la Dirección de Supervisión y Control de la DGPDP, que concluye el procedimiento de fiscalización, se establecerán, de ser el caso, las medidas que deberán ordenarse al presunto responsable en vía cautelar.

El mismo hecho de obstruir el ejercicio de la función fiscalizadora constituye una infracción considerada leve, y hacerlo en forma sistemática o suministrando documentos o información falsa o incompleta constituye una infracción grave. Igualmente, se considera una infracción grave el dar tratamiento a datos personales contraviniendo los principios establecidos en la LPDP o incumpliendo sus demás disposiciones o las de su reglamento. Asimismo, si esto último impide o atenta contra el ejercicio de los derechos fundamentales de la persona, ello se considerará una infracción muy grave.

La determinación de la existencia de infracciones es objeto del procedimiento sancionador, así como la imposición o no de sanciones y obligaciones accesorias tendientes a la protección de los datos personales. La sanción administrativa de multa se fija en función a la Unidad Impositiva Tributaria vigente a la fecha en que se cometió la infracción. El reconocimiento espontáneo de las infracciones, acompañado de acciones de enmienda, se

(14) La auditoría será externa en caso de las categorías de tratamiento complejo y crítico.

considerará atenuante que permitirá la reducción motivada de la sanción por debajo de lo previsto en la LPDP. La ejecución de la sanción de multa se rige por la ley del procedimiento de ejecución coactiva.

Conclusión

En la actualidad, el interés social por la protección de los datos personales es consecuencia del aumento del riesgo de pérdida de confidencialidad, integridad o disponibilidad debido a su tratamiento automatizado. En nuestro país, la promulgación de una ley especial que introduce el principio de seguridad obliga a los titulares de bancos de datos personales y a los encargados de su tratamiento a documentar las medidas de seguridad implementadas, tanto para la información digital como el almacenamiento de documentación no automatizada con el objetivo de disminuir o evitar el riesgo humano o técnico de adulteración, pérdida o desviación de información y cualquier tratamiento ilegal.

El ejercicio del poder que da el uso de la informática y las telecomunicaciones amenaza a la intimidad de las personas cuyos datos son procesados o transmitidos. La responsabilidad directa de la reducción de los riesgos que aquélla conlleva le corresponde a quienes los generan y los conocen; la autorregulación es la fórmula con la que los Estados cuentan para proteger la dignidad de las personas en una sociedad en la que la ciencia y la técnica dominan los procesos que generan las principales amenazas en su contra.

La normalización de los sistemas de gestión de seguridad de la información, instrumento del Derecho privado, se extiende al Derecho público con la Directiva de Seguridad de la información aprobada por la Dirección General de Protección de Datos Personales, la que dispone un conjunto de medidas organizativas, jurídicas y técnicas contra el acceso no autorizado, la alteración o pérdida de datos y el tratamiento no autorizado de éstos. La implementación de determinadas medidas de seguridad es requerida, según corresponda, a categorías establecidas en relación con el volumen de registros y ubicuidad del banco de datos, el número y calidad de datos por persona, el plazo para su tratamiento y la calidad del titular del banco de datos. Los requisitos de seguridad establecidos en la directiva documentan el cumplimiento de las medidas implementadas y fundamentarán, sin duda, los procedimientos de fiscalización por presunto tratamiento de datos contraviniendo el principio de seguridad establecido en la LPDP. El conocimiento de la naturaleza y el objeto de las medidas de seguridad de la información será útil para los abogados llamados a asistir legalmente en las cuestiones derivadas de posibles incumplimientos del principio legal. Surgido éste en el lector se cumple el propósito del artículo.