LATINOAMÉRICA

¿CÓMO ESTÁ AVANZANDO LA CIBERSEGURIDAD EN EL PERÚ? BREVE APROXIMACIÓN AL MARCO NORMATIVO

¿Cómo está avanzando la ciberseguridad en el Perú? Breve aproximación al marco normativo

El Perú no es ajeno al gran reto que representa para las organizaciones el proceso de transformación digital y que conlleva una necesaria reflexión respecto de las amenazas latentes por la potencial vulneración a la seguridad de los sistemas de información. Este artículo busca ejemplificar el marco normativo que se viene desarrollando en el país con relación a la ciberseguridad y mostrar que, si bien no es aparente, sí existe una preocupación por esta materia.

The progress of cybersecurity regulation in Peru

Peru is not excluded from the immense challenge that a process of digital transformation represents for organizations and that entails a necessary deliberation regarding the latent threats due to the potential violation of the security of information systems. This article seeks to exemplify the regulatory framework that has been developed in the country in relation to cybersecurity and evidences that, although it is not recognizable, there is a genuine concern about this matter.

Palabras clave

Ciberseguridad, Transformación digital, Protección de datos personales, Ciberataque, Internet, Información, Seguridad informática.

Key words

Cybersecurity, Digital transformation, Data protection, Cyberattack, Internet, Information, Information security.

Fecha de recepción: 20-9-2019 *Fecha de aceptación: 27-9-2019*

Existe un amplio consenso respecto del incremento global de los ciberataques, así como de la sofisticación con la que los incidentes de ciberseguridad se vienen manifestando. Y, si bien este hecho debería derivar en una toma de conciencia de los posibles daños —incluso irreparables— que podrían sufrir las empresas en el Perú, la realidad es que esta preocupación no parece estar en su agenda, al menos de forma inmediata.

La razón por la que ello ocurre quizás se encuentra en una falta de entendimiento de lo que comprende la ciberseguridad, pero también de la complejidad y retos que supone regular de manera orgánica esta materia sin dejar de atender las exigencias de llevar adelante y, a galope, una transformación digital.

En lo que respecta a la ciberseguridad, debemos partir de la base que el riesgo de sufrir un ciberataque no es un riesgo que haya de ser prevenido, atribuido y mitigado únicamente por las áreas de seguridad de la información, sino que también es un riesgo del negocio y, como tal, debe ser atendido al más alto nivel de toda organización. En efecto, los riesgos en ciberseguridad son la consecuencia natural de la transversalidad e interconectividad que vivimos; si las buscamos en nuestras operaciones e interacciones, estas acciones acarrearán costos, como develar las vulnerabilidades en nuestros sistemas. Por tanto, no cabe pensar en geografías o jurisdicciones, pues todos los que nos beneficiamos de Internet tendremos que enfrentar un ciberataque en algún momento.

Siendo ello así, proteger la infraestructura de la información y los datos no es una tarea que deba esperar a que nuestro ordenamiento jurídico desarrolle más o mejores estándares segmentados por industrias, emita una ley marco en materia de ciberseguridad o disponga sanciones económicas ante ciertos incumplimientos. Tanto el sector privado como el sector público están llamados a tomar acción y protegerse ante las amenazas externas e internas que ocurren en el ciberespacio y que pueden afectar la llamada tríada CID o triángulo de seguridad de los sistemas informáticos de toda organización: la confidencialidad, la integridad y la disponibilidad.

Ahora bien, si tomamos atención e identificamos una serie de normas que reflejan la evolución hacia lo digital que acontece en el Perú desde hace algunos años, ciertamente notaremos que no es escasa la mirada y preocupación que ha tenido la ciberseguridad en nuestro ordenamiento jurídico. Sin que las referencias que citaremos a continuación sean exhaustivas ni se encuentren en orden de importancia, mencionaremos algunos casos distintivos.

El primero de ellos data del año 2013 y se refiere a la Directiva de Seguridad que acompaña la Ley No.

García, Viviana: "¿Cómo está avanzando la ciberseguridad en el Perú? Breve aproximación al marco normativo", *Actualidad Jurídica Uría Menéndez*, 52, 2019, pp. 176-179 (ISSN: 1578-956X).

29733 —Ley de Protección de Datos Personales— y su Reglamento, aprobado mediante Decreto Supremo No. 003-2013-JUS. La Directiva de Seguridad es una herramienta que facilita el cumplimiento de la referida Ley y su Reglamento, y que se ocupa de brindar, entre otros, lineamientos para determinar las medidas de seguridad que resulten apropiadas en función de las características del tratamiento de datos personales que se efectúe.

Esta Directiva plantea una clasificación de categorías en el tratamiento de datos personales estableciendo que, para bancos de datos considerados críticos, se requiere, entre otras medidas:

(i) que toda información electrónica que contenga datos personales sea almacenada en forma segura empleando mecanismos de control de acceso y que esté cifrada para preservar la confidencialidad;

(ii) que los equipos utilizados para dichos tratamientos cuenten con *software* de protección contra *malware* para proteger la integridad de los datos personales y que dichos *softwares* de protección sean actualizados frecuentemente de acuerdo a las recomendaciones y especificaciones del proveedor, y

(iii) que los equipos utilizados para el tratamiento reciban mantenimiento preventivo y correctivo de acuerdo a las recomendaciones y especificaciones del proveedor para asegurar su disponibilidad e integridad, y que dicho mantenimiento sea realizado por personal autorizado.

El segundo caso se refiere a la Ley No. 30024, promulgada en el 2013 y reglamentada en el año 2017 mediante Decreto Supremo No. 009-2017-SA, por medio de la cual se creó el Registro Nacional de Historias Clínicas Electrónicas (RENHICE). Estas normas introdujeron en nuestro sistema legal la necesidad de regular la historia clínica electrónica, indicando que su tratamiento —que comprende el registro, almacenamiento, actualización, acceso y uso— debe realizarse en condiciones de seguridad, integralidad, autenticidad, confidencialidad, exactitud, inteligibilidad, conservación y disponibilidad. Se dispuso además que el RENHICE debe regirse por el principio de seguridad, según el cual dicho Registro y los sistemas de información de historias clínicas electrónicas se enmarcan dentro de un sistema de gestión de la seguridad de la información, que garantiza la confidencialidad y el derecho a la privacidad de los propietarios de la información clínica contenida en las historias clínicas electrónicas. Así, lo que esta regulación ha determinado es que, si bien la propiedad de la información clínica contenida en las historias clínicas no deja de pertenecerle a cada paciente, la reserva, privacidad y confidencialidad —elementos claves de la ciberseguridad— tienen que ser garantizadas por el Estado, los establecimientos de salud y los servicios médicos de apoyo.

También en el año 2013 el Congreso de la República promulgó la Ley de Delitos Informáticos, Ley No. 30096, con el propósito de prevenir y sancionar la ciberdelincuencia, es decir, las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación. Esta Ley y sus normas modificatorias, clasifican los delitos en los siguientes tipos: (i) delitos contra datos y sistemas informáticos, entre los que se incluyen el acceso ilícito, el atentado contra la integridad de datos y el atentado contra la integridad de sistemas informáticos; (ii) delitos informáticos contra la indemnidad y libertad sexuales, tales como las proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos; (iii) delitos informáticos contra la intimidad y el secreto de las comunicaciones, como la interceptación de datos informáticos; (iv) delitos informáticos contra el patrimonio, como el fraude informático; y (v) delitos informáticos contra la fe pública, como la suplantación de identidad.

Cabe resaltar que la referida Ley No. 30096 tiene además una vocación mucho más amplia al tipificar el uso de una serie de mecanismos accesorios y complementarios que son empleados por los ciberdelincuentes. De esta manera, la Ley considera también que delinquen quienes deliberada e ilegítimamente fabrican, diseñan, desarrollan, venden, facilitan, distribuyen, importan u obtienen para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier dato informático que se encuentre específicamente diseñado para la comisión de delitos informáticos.

Un par de años después, en el año 2015, el Perú reguló de manera expresa el teletrabajo al aprobar la Ley No. 30036 y, posteriormente, su Reglamento mediante Decreto Supremo No. 009-2015-TR. Al amparo de estas normas, el teletrabajo es considerado como una modalidad especial de prestación de servicios caracterizada por la utilización de tecnologías de la información y telecomunicaciones

(TIC) y, por tanto, suscita una serie de acciones que deberían realizarse en materia de ciberseguridad.

El Reglamento de la Ley No. 30036 dispone que el acuerdo por el cual se establezca la modalidad de teletrabajo debe consignar las medidas sobre la gestión y seguridad de la información derivadas del uso de los medios con que se preste el servicio bajo esta modalidad. En cuanto a los derechos del teletrabajador, indica que se le deberá garantizar una capacitación sobre los medios informáticos, de telecomunicaciones y análogos que empleará para el desempeño de la ocupación específica, así como sobre las restricciones en el empleo de tales medios, la legislación vigente en materia de protección de datos personales, propiedad intelectual y seguridad de la información. De manera consecuente, se establece que es una obligación del teletrabajador cumplir con la normativa vigente sobre seguridad de la información, protección y confidencialidad de los datos y seguridad y salud en el trabajo. Agregan también estas normas que la provisión de las condiciones de trabajo para la prestación de esta modalidad —equipos, acceso a Internet, conexiones de red, programas informáticos, medidas de seguridad de la información— obliga a quien las otorga a garantizar la idoneidad de todas ellas. Este último aspecto resulta relevante en la medida que, al referirnos a infraestructura crítica en ciberseguridad, esta no solo debe de ser pensada en sistemas informáticos, sino también en seguridad física.

Sin rango legal, pero no por ello menos relevante en cuanto a la preocupación por enfrentar con una metodología clara los riesgos derivados de los ciberataques, en el año 2016 se aprobó mediante la Resolución de Superintendencia No. 00027-2016, emitida por la Superintendencia del Mercado de Valores (SMV), el Reglamento de Gestión de Riesgo Operacional aplicable a las entidades a las que la SMV otorga autorización de funcionamiento. El Reglamento tiene como finalidad establecer lineamientos, criterios y parámetros generales mínimos que las entidades bajo la supervisión de la SMV deben observar en el diseño, desarrollo y aplicación de su gestión de riesgo operacional, de acuerdo con la naturaleza y proporcionalidad del negocio.

Tomando nota de lo señalado párrafos atrás, debe destacarse que el Reglamento dispone de manera expresa que implementar tanto un sistema de gestión de seguridad de la información como un sistema de gestión de continuidad del negocio es parte de una adecuada gestión del riesgo operacional de las entidades. En cuanto a la implementación del primero de ellos, la norma indica que este permitirá garantizar la tríada CID, así como gestionar los riesgos, incluidos los de ciberseguridad, mediante la adecuada combinación de políticas, procedimientos, controles, estructura organizacional y herramientas informáticas especializadas. De otro lado, en lo que respecta al sistema de gestión de continuidad del negocio, la citada norma establece que, ante la ocurrencia de eventos que puedan crear una interrupción o inestabilidad de las operaciones de la entidad, este sistema tendrá como objetivo brindar respuestas efectivas para que la operatividad del negocio continúe de una manera razonable.

Si bien el Reglamento desarrolla ampliamente una serie de nociones en ciberseguridad, lo que es notable es que incluye, dentro de los reportes periódicos de indicadores clave de riesgo operacional que las entidades deben presentar a la SMV, el reporte trimestral de "Seguridad de la Información" que comprende las vulnerabilidades identificadas, pero también la inversión en ciberseguridad. Este último aspecto cobra ciertamente relevancia en la medida que gestionar riesgos de ciberataques en toda organización requiere que todo un compromiso a nivel gerencial y de dirección se vea reflejado en la aprobación de los presupuestos y de las inversiones necesarias.

Desde el Estado, los esfuerzos recientes por regular la ciberseguridad se vienen manifestando a través de la Secretaría de Gobierno Digital (SeGDi), creada en el año 2017. Según lo dispuesto por el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, la SeGDi es el órgano de línea, con autoridad técnico-normativa a nivel nacional responsable de formular y proponer políticas nacionales y sectoriales, planes nacionales, normas, lineamientos y estrategias en materia de informática y gobierno electrónico. Así, en el marco de sus funciones, y tomando en cuenta el Programa de Implementación de las Recomendaciones del Estudio de Gobernanza Pública trabajado con la Organización para el Crecimiento y Desarrollo Económicos (OCDE), la SeGDi viene impulsando el marco jurídico que acompaña los procesos de transformación digital en la Administración pública.

A manera de conclusión cabe indicar que, a finales del mes de julio de 2019, existen dos proyectos de ley que han sido presentados al Área de Trámite Documentario del Congreso de la República el pasado mes de abril de 2019. Uno de ellos es el proyecto de Ley de Ciberdefensa, que tiene como

propósito establecer un marco normativo en materia de ciberdefensa del Estado peruano y que regulará las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa. Su ámbito de aplicación se circunscribe a la ejecución de operaciones de ciberdefensa frente a las amenazas o ataques que atenten contra la seguridad nacional.

El segundo es el proyecto de Ley que promueve la seguridad informática en el Perú y la conformación de un Consejo Nacional de Ciberseguridad. Lo relevante de este segundo proyecto es que su objeto es promover la seguridad informática en todo el territorio nacional bajo los principios de (i) colaboración multidisciplinaria multisectorial e interinstitucional, (ii) respeto a los derechos humanos y (iii) desde un enfoque basado en gestión de riesgos. Asimismo, es significativo que este proyecto proponga regular la obligatoriedad de las entidades de la Administración pública y privada de comunicar los incidentes, ataques y/o vulneraciones cibernéticas que hayan sufrido y, más aún, las acciones correspondientes tomadas para su solución, dentro de un plazo que será establecido por un Comité de Respuesta ante Ciberdelincuencia (CORECY). El proyecto propone la creación del CORECY como una dependencia del Consejo Nacional de Ciberseguridad (CONACY), organismo este último conformado no solo por entidades del sector público, sino también del sector privado.

Viviana García (*)

(*) Socia de Philippi Prietocarrizosa Ferrero DU & Uría (Perú).