Seguridad de la información

Sinopsis de políticas

8 Principios rectores de la transformación digital del sector salud

Caja de herramientas de transformación digital

OPS Organización Panamericana de la Salud
Organización Mundial de la Salud Américas

ORGANIZACIÓN, COORDINACIÓN Y DESARROLLO

Departamento de Evidencia e Inteligencia para la Acción de Salud (EIH) de la Organización Panamericana de la Salud (OPS), en colaboración con el Centro de Implementación e Innovación en Políticas de Salud (CIIPS), parte del Instituto de Efectividad Clínica y Sanitaria (IECS), Centro Colaborador de la OPS.

AGRADECIMIENTO

La OPS desea manifestar su agradecimiento al Gobierno de Estados Unidos de América por la contribución financiera que hizo posible el desarrollo de este importante producto que forma parte de una caja de herramientas de apoyo al fortalecimiento de la implementación de la iniciativa regional de telesalud en la lucha contra las enfermedades no transmisibles.

RECONOCIMIENTO

La OPS reconoce y agradece el apoyo de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID), de la Agencia de Estados Unidos para el Desarrollo Internacional (USAID), del Gobierno de Canadá, del Banco Interamericano de Desarrollo (BID), así como a la red de expertos que apoyan la iniciativa sobre los sistemas de información para la salud de la OPS.

Índice

Resumen

Uno de los ocho principios rectores para la transformación digital del sector salud promovidos por la Organización Panamericana de la Salud (OPS) es la **seguridad de la información**. Este documento de política presenta conceptos clave, líneas de acción recomendadas e indicadores para su monitoreo con el objetivo de avanzar en la seguridad de la información.

De acuerdo con la definición de la OPS, este principio se propone **establecer mecanismos de confianza y seguridad de la información en el entorno digital de la salud pública**. "Adoptar instrumentos normativos sobre el tratamiento y la protección de datos sensibles de salud, así como pautas y normas internacionales de seguridad para los sistemas de información centrados en el paciente. Estos sistemas deben implantarse respetando los derechos relativos a la salud, a fin de generar una 'cultura de manejo de datos seguros y confiables', entendida como el equilibrio entre la necesidad de acceder a los datos y la privacidad" (*1*).

En el marco de la salud, la información que hay que proteger no solo reviste carácter de bien, sino que conlleva dimensiones éticas, legales y técnicas que deben ser resguardadas. La seguridad de esos datos se define en términos de la norma ISO como "preservación de la confidencialidad, integridad y disponibilidad de la información". De esta definición se desprenden los tres elementos que, fundamentalmente, deben considerar los mecanismos de seguridad para resultar funcionales a las organizaciones en las cuales se implemente.

La seguridad de la información se establece, así, como una base fundamental en el desarrollo exitoso de cualquier organización, institución o sistema, implicando las estrategias, planificaciones y desarrollos que se lleven a cabo para proteger la información de los riesgos de ataques que posibiliten el uso indebido o ilegal del bien en custodia.

En este documento se recorre el estado actual de la seguridad de la información y se brindan recomendaciones y líneas de acción y monitoreo de la seguridad. Es importante focalizarse en un plan de acción que considere como líneas indisociables de su eficacia desarrollar un plan de seguridad y protección de datos enmarcado en políticas públicas y ajustado a derecho; contar con una estructura de control sobre el flujo de información en salud, con elementos de pautas de seguridad informática y riesgos asociados; establecer mecanismos de monitoreo orientados a la detección de incidentes; generar instancias de archivo de consentimiento informado; centralizar las certificaciones de seguridad, y promover y elaborar planes de formación continua y desarrollo del personal.

Además, es preciso contar con instrumentos normativos en relación con la protección de datos sensibles en el área de la salud y pautas internacionales orientadas a la seguridad de los sistemas de información para la salud (SIS), con el fin de fomentar el buen uso de datos en términos de un equilibrio entre el acceso y la privacidad.

Palabras clave: *seguridad, ética, accesibilidad, confidencialidad, datos sensibles, normativas.*

Introducción

"Es también imperativo proteger la información de salud sensible, y por consiguiente, es necesario colaborar y crear en conjunto mecanismos para preservar la confidencialidad y la seguridad de la información personal en el entorno de la salud pública digital y, simultáneamente, promover el acceso y la transparencia en la información y el conocimiento". Declaración de la Organización Panamericana de la Salud durante la Conferencia de Alto Nivel sobre Sistemas de Información para la Salud, febrero de 2021.

Pensar en la seguridad de la información implica tomar en cuenta qué información se pone a disposición, por qué medios, a quienes, dónde se aloja, cómo es el tratamiento de esos datos, bajo qué regulaciones y marcos normativos está inserto (o es necesario crear), cómo propiciar un escenario y circuitos en los que se respeten los derechos relativos a la salud y, a su vez, asumir el desafío de que exista un acceso fluido y transparente a la información velando al mismo tiempo por la confidencialidad y privacidad de la información sensible, tal como es aquella que resulta del vínculo de las personas con el sistema de salud.

Los desafíos que trae aparejada la búsqueda de estrategias robustas y un equilibrio alrededor de la necesidad de acceder a información sanitaria y, a la vez, contemplar las particularidades de la privacidad y la seguridad inherentes a los datos sensibles invita a pensar en varias dimensiones para abordar el principio de seguridad de la información.

Además de la adopción de instrumentos normativos sobre el tratamiento y la protección de datos sensibles de salud, es importante conocer e implementar las pautas y normas internacionales de seguridad para los sistemas de información centrados en el paciente y poner el foco en los aspectos más específicos en escenarios jurisdiccionales, no circunscribiéndose exclusivamente a una dimensión técnica, sino creando y fortaleciendo un camino hacia una cultura de manejo de datos seguros y confiables.

Las tecnologías digitales pueden contribuir a aumentar el acceso a los grupos poblacionales en mayor situación de vulnerabilidad en materia de salud, siendo necesario apelar al desarrollo del capital humano y de la infraestructura que permitan utilizar las tecnologías digitales de forma inclusiva, ética y segura. En este escenario, la seguridad de la información es un principio central.

El abordaje integral y la revisión de la seguridad de la información contempla el establecimiento de mecanismos de confianza en el entorno digital de la salud pública, considerando dimensiones éticas, técnicas y legales.

Partiendo de considerar a la información como un activo esencial para las actividades y la necesidad de una protección adecuada, es oportuno destacar en primera instancia que los datos de salud se consideran información sensible; el *habeas data* es una acción que permite a las personas conocer qué datos personales suyos son almacenados y utilizados por terceros, y optar por la posibilidad de actualizarlos, modificarlos o borrarlos. Por ejemplo, en Argentina, se toma en cuenta el marco legal nacional destacando la mención al uso de información en la Constitución Nacional y la existencia de un grupo de leyes que aborda específicamente la protección de datos personales, los derechos del paciente en relación con los profesionales y las instituciones de salud, y el acceso a la información pública.

A su vez, la Organización Mundial de la Salud (OMS) ha publicado lineamientos que se refieren a aspectos de salud digital y ciberseguridad, al desarrollo de ecosistemas de salud interoperables y a la elaboración de requisitos jurídicos que garanticen códigos éticos para salvaguardar la seguridad del paciente y sus datos. Por su parte, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) ha publicado advertencias y recomendaciones de buenas prácticas en seguridad de la información, en particular sobre la evolución y tendencia de las amenazas (*2*). La Red Iberoamericana de Protección de Datos busca promover desarrollos normativos y políticas necesarios para garantizar la regulación avanzada del derecho a la protección de datos personales (*3*). Por último, las normas ISO establecen los controles y estrategias necesarias para eliminar o minimizar riesgos (*4*).

Tomando como referencia experiencias exitosas y la detección de patrones para avanzar en la implementación, se destacan tres dimensiones y condiciones necesarias:

- La definición de una política de seguridad de la información para los distintos actores u organismos.
- Una garantía de convivencia de las distintas áreas en una sola red.
- La definición de un marco normativo que regule la aplicación y cumplimiento de las normativas por las partes intervinientes que participen o deseen participar de la red.

El éxito en la ejecución de las líneas de acción se vincula a la clara definición de instancias y establecimiento de objetivos contando con el aval y participación activa de la multiplicidad de actores involucrados de una manera cohesiva y articulada.

Estado actual e identificación de brechas

El primer aspecto que hay que destacar es la **heterogeneidad en relación con los marcos normativos existentes en los países de la región**. Se observan distintos estadios de desarrollo de normativas (*5*): Colombia y Venezuela (Estado Plurinacional de) cuentan con menciones sobre esta temática en sus marcos constitucionales. Y países como Argentina, Brasil, Chile, Perú, Paraguay y Uruguay disponen, además, de leyes específicas sobre el tratamiento de datos personales.

Además, la OPS insta a identificar la necesidad de desarrollar normativas que busquen un equilibrio entre accesibilidad y privacidad apuntando a la protección del individuo, sin retrasar o bloquear el desarrollo de tecnologías de salud digital (*1*).

Los lineamientos internacionales constituyen referencias y guías. Sin embargo, resulta conveniente generar marcos propios en las estrategias nacionales como complemento a las normas y guías internacionales sobre protección de datos. Es posible detectar dificultades específicas en algunos escenarios nacionales vinculadas a la falta de mecanismos que garanticen la seguridad de los datos, la existencia de heterogeneidades jurisdiccionales respecto a las regulaciones y la falta de acuerdos internacionales respecto a los estándares.

En segundo lugar, es necesario desarrollar y establecer políticas públicas que incorporen un plan de seguridad y protección de los datos de salud, con foco en perfiles de acceso en función de las acciones que deba realizar el usuario.

En relación con ello, se presenta la dificultad asociada al **entorno cambiante de la seguridad de los datos, e incluso la falta de información (en términos de cifras y de caracterización de incidentes de ciberseguridad en América Latina)**. Este tipo de análisis y monitoreo existe en la Unión Europea a partir de la ENISA (*2*), la cual brinda información actual sobre la evolución y la tendencia de las amenazas, y ayuda a las partes interesadas a reconocerlas y desarrollar estrategias de respuesta. Brinda, asimismo, una descripción general de las amenazas a sistemas, los agentes de las amenazas, sus tendencias actuales y las emergentes. Este tipo de información aún no se ofrece en la Región de América Latina.

En tercer lugar, existe un **débil desarrollo de estrategias de capacitación dirigida a los actores involucrados en el flujo de información de salud sobre pautas de seguridad informática y riesgos asociados**. Su existencia permitiría fortalecer la formación en recursos humanos especializados que puedan resolver los incidentes de seguridad, y fomentar el reconocimiento de las Leyes Generales de Protección de Datos (*5*) como instrumentos iniciales para promover la discusión sobre las responsabilidades personales y de las organizaciones. En este sentido, un documento publicado por la Red Iberoamericana de Protección de Datos busca brindar un modelo de referencia para la regulación futura en la región y revisión de las normas vigentes, en relación con el derecho de protección de datos en países que aún no cuentan con marcos normativos, o que deban actualizar las legislaciones existentes. (*3*).

Asimismo, **aún no se cuenta con mecanismos de monitoreo que permitan detectar incidentes de seguridad en los sistemas de información para la salud.** Ante ello, es preciso fortalecer la estrategia nacional de ciberseguridad. En la materia, la principal referencia son las normas de la Organización Internacional de Normalización (4) que, si bien establece los controles y estrategias necesarias para eliminar o minimizar riesgos, no se adapta a contextos locales.

Por último, **la población aún no dimensiona sus derechos y responsabilidades en relación con sus datos personales y a disponer de instancias de consentimiento informado en cuanto al acceso, registro y salvaguarda de la información sensible**. Por ejemplo, en Argentina, la Ley 26.5296 sancionada en 2009 trata sobre los Derechos del Paciente en su Relación con los Profesionales e Instituciones de la Salud y establece los derechos esenciales en la relación entre el paciente y el o los profesionales de la salud, el o los agentes del seguro de salud, y cualquier otro efector. Entre ellos, se menciona la confidencialidad, en tanto el paciente tiene derecho a que toda persona que participe en la elaboración o manipulación de la documentación clínica, o bien tenga acceso al contenido de esta, guarde la debida reserva, salvo expresa disposición en contrario emanada de autoridad judicial competente o autorización del propio paciente. Otros ejemplos se refieren a la Ley Orgánica 459 del 2021 de Protección de Datos Personales de Ecuador (6) o la Ley de Protección de Datos Personales o Ley 581 de 2021 de Colombia (7).

No obstante, **aún constituye un desafío asumir el rol del paciente como titular de los datos y fomentar su participación activa en el principio de seguridad**. Los usuarios no han incorporado aún el derecho a exigir protección sobre su información, las correctas aplicaciones de resguardo de los datos y la continuidad y solidez del seguimiento precautorio de anomalías.

Líneas de acción

La OPS propone a la seguridad de la información como uno de los ocho principios rectores de la transformación digital del sector de la salud (1, 8, 9), donde se propician los siguientes lineamientos de acción:

1. Contar con instrumentos normativos que regulen el tratamiento y el acceso a los datos de salud desde los ejes de privacidad, confidencialidad y seguridad de la información.

2. Formular políticas públicas que incorporen un plan de seguridad y protección de los datos de salud, definiendo perfiles de acceso en función de las acciones que deba realizar el usuario.

3. Capacitar activamente a todos los actores involucrados en el flujo de información de salud sobre pautas de seguridad informática y riesgos asociados.

4. Articular mecanismos de monitoreo que permitan detectar incidentes de seguridad en los sistemas de información para la salud.

5. Disponer de instancias de consentimiento informado en cuanto al acceso, registro y salvaguarda de la información sensible.

6. Habilitar servicios centralizados de certificación de seguridad de datos sensibles de salud mediante tecnologías de certificación de cadena de bloques (*blockchain*), entre otros.

7. Adoptar planes de comunicación para concientizar a la población sobre sus derechos y responsabilidades sobre sus datos personales.

8. Actualizar las normas vigentes de protección de datos (muchas de las cuales se crearon antes de la era digital) con nuevos temas como la ciberseguridad.

Teniendo en cuenta la complejidad que supone lograr la seguridad de la información, las líneas de acción recomendadas abarcan aspectos técnicos, legales, de planificación y de gestión tanto por parte de las organizaciones como de los gobiernos. Considerar la seguridad desde el comienzo, invitando a romper la lógica en la que aparece solamente vinculada a riesgos, fallas o en una instancia posterior a la planificación e implementación, hará que las mismas sean más organizadas, escalables y eficientes, tanto a nivel institucional al planificar los circuitos, como a nivel gubernamental para crear un escenario lo más sólido posible.

A continuación, se enumeran algunas recomendaciones que complementan las líneas de acción establecidas por la OPS en su documento sobre los *8 principios rectores de la transformación digital del sector de la salud* útiles para distintos actores vinculados con la seguridad de la información, desde las instituciones hasta los organismos de Gobierno:

1. CONTAR CON INSTRUMENTOS NORMATIVOS QUE REGULEN EL TRATAMIENTO Y EL ACCESO A LOS DATOS DE SALUD DESDE LOS EJES DE PRIVACIDAD, CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN

Evaluar y definir un marco normativo que establezca las normas de aplicación para los participantes de la red. Este marco debe establecer claramente las pautas mínimas de cumplimiento, así como explicitar con claridad las sanciones o penalidades a las que se exponen los distintos actores u organismos respecto del acceso a datos desde los ejes de confidencialidad, privacidad y seguridad de la información.

2. DESARROLLAR UNA ESTRUCTURA DE CONTROL SOBRE EL FLUJO DE INFORMACIÓN EN SALUD, CON ELEMENTOS DE PAUTAS DE SEGURIDAD INFORMÁTICA Y RIESGOS ASOCIADOS

- Generar mecanismos de auditorías que permitan realizar un control periódico de los distintos organismos participantes de la red de modo que se garantice que cumplen con las normas de aplicación para los participantes de la red.

3. ESTABLECER MECANISMOS DE MONITOREO ORIENTADOS A LA DETECCIÓN DE INCIDENTES, ASÍ COMO AL CHEQUEO DEL CORRECTO CUMPLIMIENTO DE LOS ESTÁNDARES Y CONDICIONES DE ACCESO Y TRATAMIENTO DE LA INFORMACIÓN

- Definir un plan de contingencia y el funcionamiento de una unidad que coordine las emergencias en la red de teleinformática y que permita manejar los incidentes de seguridad que pudieren surgir, así como alertar a los participantes de dicha red para poder neutralizar de manera preventiva o correctiva dichas amenazas. Esta unidad debería actuar como repositorio de la información de dichos incidentes y difundir las herramientas y técnicas de defensa que deben aplicarse en el marco de la red.

4. ESTABLECER HERRAMIENTAS E INSTANCIAS DE CONSENTIMIENTO INFORMADO DEL ALMACENAMIENTO Y RESGUARDO DE LA INFORMACIÓN SENSIBLE

- Contemplar las características de las plataformas e interfaz de acceso y disponibilización de información y enmarcarlas en un circuito que implica un compromiso formal y la firma de consentimientos informados y convenios de confidencialidad que los usuarios deberán cumplir antes de acceder a la información consolidada.

- Se recomienda, a su vez, el monitoreo y seguimiento de esos accesos con su respectiva validación.

5. CENTRALIZAR LAS CERTIFICACIONES DE SEGURIDAD

- Crear servicios que permitan manejar de manera centralizada los aspectos inherentes a la certificación de los datos sensibles de salud mediante la utilización de tecnologías de certificación de cadena de bloques (blockchain).

- Generar los mecanismos que permitan la actualización del marco normativo ante la aparición de nuevas tecnologías o puntos ciegos que no hubieren sido contemplados, asegurando el cumplimiento de los estándares de seguridad.

6. ELABORAR Y EJECUTAR PLANES DE COMUNICACIÓN Y CAPACITACIÓN SOBRE DERECHOS Y RESPONSABILIDADES RESPECTO A LOS DATOS PERSONALES

- Desarrollar documentos y espacios de formación, difusión y concientización para transmitir de manera asertiva conocimientos sobre el marco legal vigente. El conocimiento por parte de los actores involucrados respecto a sus derechos y obligaciones es principal: de nada sirve la robustez técnica o de circuitos sin el respaldo de definiciones formales respecto a los derechos, obligaciones, reglas de juego y buenas prácticas que deben cumplir las personas e instituciones involucradas en el ciclo de vida de la información.

- A nivel gubernamental, explicitar los derechos de cada persona respecto a su información y las obligaciones por parte de las instituciones de realizar un correcto tratamiento. Esta debe ser una dimensión presente en la agenda.

7. ACTUALIZAR NORMAS Y HERRAMIENTAS VIGENTES VINCULADAS A LA PROTECCIÓN DE DATOS

- La aparición de nuevas tecnologías y escenarios complejos requiere tener presente que no nos encontramos ante situaciones estáticas, sino que es necesaria la capacidad de generar ciclos de mejoras continuas y actualización tanto de la dimensión técnica como normativa y ética que vayan integrando todos los nuevos elementos que atraviesan al principio de seguridad. No basta con definir una serie de medidas o una planificación estática, sino también atender aquellas situaciones que quedan provisoriamente no contempladas e ir ajustando y monitoreando permanentemente los procesos.

• En el caso de los gobiernos, revisar la vigencia o caducidad de las normativas que afectan a estos circuitos para modificar o impulsar la creación o adhesión a nuevos marcos normativos.

8. FORTALECER LA ARTICULACIÓN INTRA E INTERINSTITUCIONAL

• La articulación es otro punto central. Desde una perspectiva interna a nivel institucional, la seguridad de la información es un elemento cohesivo e integrado con el resto de los principios rectores de la transformación digital en la salud. Si dentro de una organización intervienen varias áreas, debe propiciarse la existencia de una cohesión respecto a cómo tratar con la carga, almacenamiento, solicitudes y circuitos para la disponibilización. Desde una perspectiva externa, es menester el conocimiento del escenario jurisdiccional, nacional e internacional en el que está enmarcada la seguridad de la información para el correcto cumplimiento y consideración de las premisas y obligaciones que hay que cumplir.

• La creación de espacios y mesas de trabajo con otras instituciones y áreas de gobierno permite robustecer y fortalecer los acuerdos, y se recomiendan iniciativas gubernamentales para convocar a organismos públicos que traten con información para profundizar en la dimensión

•

de la seguridad, siendo aquellos involucrados en el ámbito sanitario un caso particular por las características de los respectivos datos.

9. DEFINIR REGLAS CLARAS RESPECTO AL FLUJO DE INFORMACIÓN: CARGA Y DISPONIBILIZACIÓN

• En lo que respecta a la carga y a las características de los datos, un llamado a la acción importante se refiere a lograr la referencia unívoca de la identidad de los usuarios y la creación de credenciales y perfiles de habilitación para el uso y acceso a los sistemas, capacitando activamente a los actores involucrados acerca de las pautas de seguridad informática, los riesgos asociados y la calidad de los datos ingresados.

• Las piezas de información o información cruda" que resultasen de esta carga deben analizarse exhaustivamente en sus características (nivel de agregación, nominalización, contenido de información sensible) y, a partir de esto, definir quién puede acceder y en qué formato, a través de qué medio o plataforma. Es probable que previamente se necesite un tratamiento de esos datos, anonimizando y eliminando posibilidades de identificadores indirectos.

Indicadores de monitoreo

Con el objetivo de avanzar en el desarrollo y la implementación de la seguridad en la información en la salud, se proponen los siguientes indicadores. Es importante aclarar que no se trata de un listado exhaustivo, sino que cada país o región puede incorporar otros indicadores, definir el nivel de desagregación necesario y la frecuencia de medición.

INDICADORES TRANSVERSALES A LOS 8 PRINCIPIOS RECTORES PARA LA TRANSFORMACIÓN DIGITAL EN SALUD.

- Existencia de una estrategia nacional de salud digital establecida mediante un marco normativo.
- Existencia de estructura organizativa gubernamental que lidere la estrategia de transformación digital en salud.
- Existencia de presupuesto destinado a una agenda digital que contemple recursos humanos y tecnología necesaria.

INDICADORES ESPECÍFICOS DE SEGURIDAD DE LA INFORMACIÓN

- Identificar indicadores para el monitoreo de la seguridad de la información resulta clave para realizar un seguimiento de manera fluida y eficaz, y comprobar que las condiciones que garantizan el correcto almacenamiento, acceso y tratamiento de los datos se cumplan o se ajusten debidamente.
- La instancia de monitoreo de la protección de datos personales requiere elementos organizados y coordinados que permitan alertar ante riesgos potenciales y hacer frente a los incidentes de seguridad que podrían atentar contra la información de los usuarios. Es recomendable que esta sea una instancia planificada y desarrollada a la par que la estrategia de implementación de sistemas de información para la salud, y no una mera adaptación a las características dadas de cada sistema. Debe constituir un elemento principal en la planificación que oficie de estímulo a la estructuración y organización e influya positivamente en la solidez y robustez de la estrategia de seguridad de la información.
- A continuación, se enumeran las recomendaciones y sugerencias vinculadas con los ejes centrales del monitoreo, el bregar por la privacidad, la confidencialidad, la seguridad y el cumplimiento de las normas.

1. Contar con instrumentos normativos que regulen el tratamiento y el acceso a los datos de salud desde los ejes de la privacidad, la confidencialidad y la seguridad de la información.

- Existencia de un marco normativo que establezca las pautas de cumplimiento de la confidencialidad, la privacidad y la seguridad de la información, así como las sanciones o penalidades.
- Existencia de un mecanismo de monitoreo del marco normativo con una frecuencia determinada que permita identificar faltas y omisiones, señalar necesidades de modificaciones y regular aspectos no contemplados.

2. Desarrollar una estructura de control sobre el flujo de información de salud, con elementos de pautas de seguridad informática y riesgos asociados.

- Existencia de un organismo de gobierno responsable de velar por la ciberseguridad en el sector de la salud y que coordine las emergencias en la red de teleinformática.
- Existencia de circuitos definidos para el monitoreo y actuación frente a incidentes.

3. Establecer mecanismos de monitoreo orientados a la detección de incidentes, así como a la comprobación del correcto cumplimiento de los estándares y condiciones de acceso y tratamiento de la información.

- Estrategia de monitoreo definida para el seguimiento de la actividad de los usuarios de la red.
- Existencia de un repositorio de información sobre incidentes.

4. Establecer herramientas e instancias de consentimiento informado del almacenamiento y resguardo de la información sensible.

- Número de convenios de confidencialidad firmados entre las partes.
- Número de consentimientos informados firmados.

5. Centralizar las certificaciones de seguridad.

- Número de servicios creados que permitan manejar de manera centralizada la certificación de los datos sensibles de salud mediante la utilización de tecnologías de certificación de cadena de bloque (blockchain).

6. Elaborar y ejecutar planes de comunicación y capacitación sobre derechos y responsabilidades respecto a los datos personales.

- Número de documentos difundidos sobre derechos y responsabilidades acerca de los datos personales.
- Existencia de espacios de formación sobre derechos y responsabilidades acerca de los datos personales.
- Campañas de difusión y concientización para transmitir de manera asertiva conocimientos sobre el marco legal vigente.

7. Actualizar normas y herramientas vigentes vinculadas a la protección de datos.

- Estrategia de actualización de las normativas definidas.

8. Fortalecer la articulación intra e interinstitucional.

- Existencia de espacios y mesas de trabajo entre distintas instituciones y áreas de gobierno, con inclusión de los usuarios.

9. Definir reglas claras respecto al flujo de información: carga y disponibilización.

- Existencia de una referencia unívoca de la identidad de los usuarios y la creación de credenciales y perfiles de habilitación para el uso y acceso a los sistemas.
- Número de capacitaciones a los actores involucrados acerca de las pautas de seguridad informática, riesgos asociados y calidad de los datos ingresados.

Recomendaciones generales

Sin desestimar el protagonismo de la dimensión técnica, es fundamental que, a la hora de desarrollar sus políticas de seguridad de la información, los decisores consideren los siguientes aspectos:

- El rol del paciente como titular de los datos y su participación activa en el principio de seguridad de la información.
- La necesidad de un abordaje integral, transversal y multidisciplinario de acuerdo con roles específicos dentro de las organizaciones.
- Poner énfasis en la difusión y concientización para que los distintos actores de la red tengan conocimiento del marco legal vigente.
- Garantizar la integridad de los datos y su disponibilización a los distintos actores de la red.
- El desarrollo de marcos normativos adecuados. Si bien existen acuerdos y consenso alrededor de las referencias normativas, cabe destacar la conveniencia de generar marcos propios nacionales o jurisdiccionales que contemplen las particularidades de los circuitos y sistemas involucrados.
- El carácter sensible de los datos resultantes de las interacciones de las personas con el ámbito sanitario requiere el desarrollo de herramientas, plataformas y estrategias con un diseño específico que contemple la correcta identificación de quienes intervienen y participan.
- En ese sentido, se recomienda el desarrollo de estrategias integrales que faciliten y fomenten el aprovechamiento del dato en tantas acciones positivas sea posible sin comprometer la seguridad y derechos de su titular.

Bibliografía y recursos

1. Organización Panamericana de la Salud. 8 principios rectores de la transformación digital del sector de la salud: Un llamado a la acción panamericana. Washington, D.C.: OPS; 2021. Disponible en: https://iris.paho.org/bitstream/handle/10665.2/53730/OPSEIHIS210004_spa.pdf.
2. Agencia de la Unión Europea para la Ciberseguridad. Acerca de la ENISA. Heraclión: ENISA; 2021. Disponible en: https://www.enisa.europa.eu/about-enisa/about/es.
3. Red Iberoamericana de Protección de Datos. Recomendaciones de La Red Iberoamericana de Protección de Datos (RIPD). Para el tratamiento de datos personales sobre la salud en tiempos de pandemia. Disponible en: https:// salud-en-pandemia.pdf.
4. Organización Internacional de Normalización. Ginebra: ISO; 2020. Disponible en: https://www.iso.org/home.htmlPlazzotta F, Sommer JA. Informática en salud orientada a la comunidad. En: Luna D, de Quirós FGB (eds.). Buenos Aires: Hospital Italiano de Buenos Aires; 2018.
5. Presidencia de la Nación de Argentina. Ley 26.529. Derechos del Paciente en su Relación con los Profesionales e Instituciones de la Salud. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/160000-164999/160432/norma.htm.
6. Gobierno del Ecuador. Ley Orgánica 459. Protección de Datos Personales. Quito: Gobierno del Ecuador; 2021.
7. Gobierno de Colombia. Ley 1.581. Protección de Datos Personales de Colombia. Bogotá: Gobierno de Colombia; 2012. Disponible en: https://www.funcionpublica.gov.co/eva/ gestornormativo/norma.php?i=49981.
8. Organización Panamericana de la Salud. Hoja de ruta para la transformación digital del sector de la salud en la Región de las Américas [resolución CD59/6]. 59.o Consejo Directivo de la OPS, 73.a Sesión del Comité Regional de la OMS para las Américas; 20 al 24 de septiembre del 2021. Washington, D.C.: OPS; 2021. Disponible en: https://www.paho.org/es/documentos/cd596-hojaruta-para-transformacion-digital-sector-salud-region-americas
9. Organización Panamericana de la Salud. Plan de Acción para el fortalecimiento de los sistemas de información para la salud 2019-2023 [resolución CD57/9]. 57.o Consejo Directivo de la OPS, 71.a sesión del Comité Regional de la OMS para las Américas; 30 de septiembre al 4 de octubre del 2019 Washington, D.C.: OPS; 2019. Disponible en: https://iris.paho.org/handle/10665.2/51617?locale-attribute=es.

OPS/EIH/IS/23-0016

OPS Organización Panamericana de la Salud
Organización Mundial de la Salud
Oficina Regional para las Américas