Universidad del Rosario: una mirada integral a la seguridad y privacidad de los datos personales en las instituciones de educación superior.

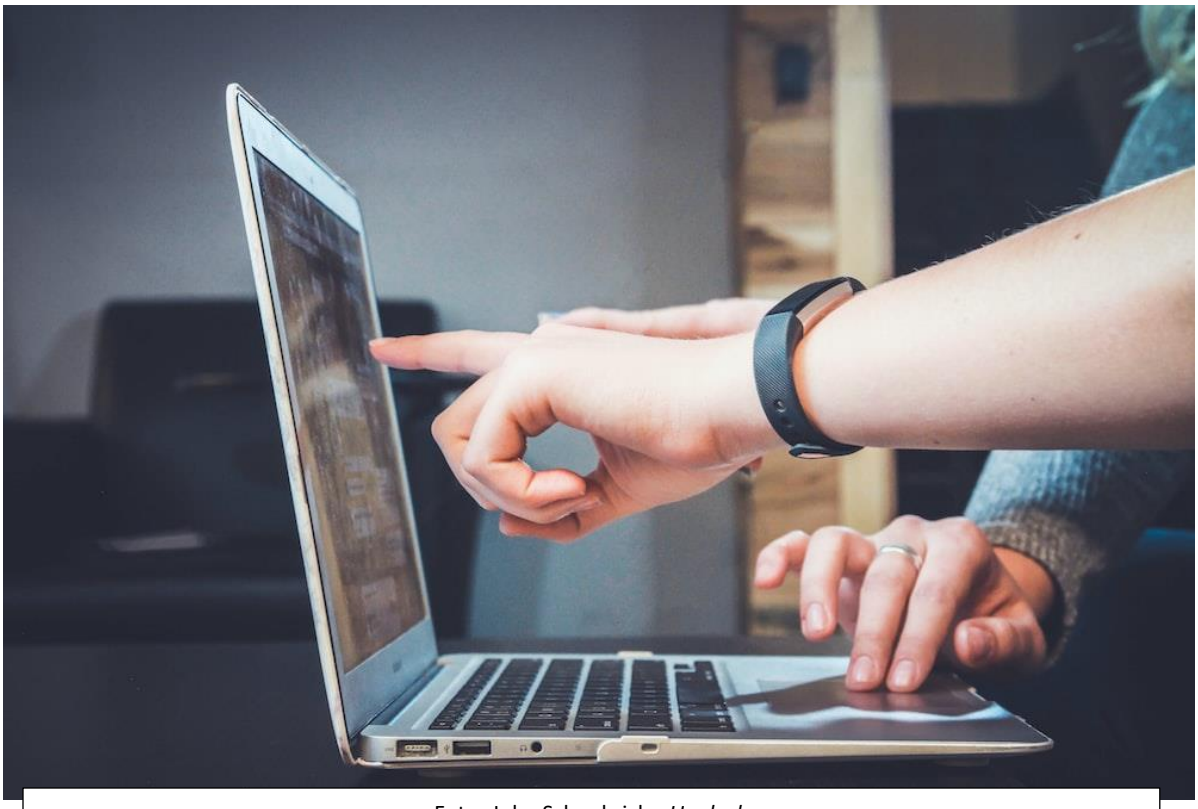

Foto: John Schnobrich - *Unplash*

Dirección de Planeación y Efectividad Institucional de la Universidad del Rosario

En Colombia, las instituciones de educación superior mantienen continuo relacionamiento con aspirantes, estudiantes, egresados, empleados, profesores, entre otros roles. Esto con el fin de, en el marco de sus funciones como son la enseñanza, investigación y extensión, recolectar, almacenar, usar, y circular datos personales que permitan entre otros puntos, identificar al titular y dar cumplimiento a la prestación del servicio de educación superior.

Bajo este contexto, la publicación de la Ley 1581 de 2012 conocida como la Ley de protección de datos personales y su reglamentación, hizo que el sector educativo asumiera el reto de construir e implementar estrategias que facilitaran el cumplimiento al derecho de las personas de conocer, actualizar, rectificar y eliminar la información recopilada en las bases de datos.

Para enfrentar este reto, en el 2013 la Universidad del Rosario se enfocó en tener una mirada integral en las diferentes aristas que se debían involucrar. Aristas como las personas, los procesos y la tecnología. Esto ha representado la oportunidad de ser referentes y evolucionar desde el buen manejo y uso de los datos personales a una visión holística 360 del dato, entendido como su ciclo de vida y tratamiento desde las personas, los procesos, lo tecnológico y jurídico asegurando la confidencialidad, integridad y disponibilidad de los datos personales.

Con la publicación de la ley, la Universidad del Rosario implementó: la política de tratamiento de datos, procedimientos para dar respuesta a las consultas y reclamos y la designación de un responsable encargado de gestionar las solicitudes presentadas por los titulares de los datos, tema que se lideraba desde la Sindicatura. En el año 2018, la Superintendencia de Industria y Comercio (SIC) amplía el alcance del Registro Nacional de Bases de Datos y de esta forma la Universidad del Rosario se convierte en un sujeto que debe realizar la inscripción de sus bases.

Para ese año, la Universidad contaba con la documentación y los procesos que se requerían para el cumplimiento de la normatividad. No obstante, se debían adoptar rápidamente nuevas estrategias que permitieran ir más allá de lo exigido por ley. Esto incluía, principalmente, la apropiación de la protección de los datos en estudiantes, profesores, empleados, investigadores y la articulación de nuevos actores para tener una visión holística del dato.

En este orden de ideas y luego de un análisis a fondo acerca del replanteamiento de la estrategia del área a liderar la protección de los datos personales en la Universidad, se hace el nombramiento de un área de Rectoría, siendo así la Dirección de Planeación y Efectividad Institucional quien asume esta responsabilidad. La Dirección se encarga de liderar los procesos y proyectos para la consecución de los objetivos estratégicos de la Universidad, así como apoyar la toma de decisiones estratégicas con el fin de acelerar la dinámica y la efectividad institucional, y por esto se toma principalmente la decisión de crear el cargo de Oficial de Seguridad de la Información y Datos Personales. Un cargo capaz de articular la Misión y Visión de la Universidad con la protección de los datos, la seguridad de la información, la normatividad y generación de acciones que preserven la seguridad y privacidad de los datos y la información.

Con el liderazgo del Oficial de Seguridad de la Información y Datos Personales, se consolidó el comité estratégico en protección de datos personales, con directivos de las áreas de Gestión Humana, Jurídica, Tecnología, Procesos, Planeación estratégica y Financiera. El comité es el mayor órgano responsable de asegurar el cumplimiento normativo y dar respuestas a las dinámicas del sector educativo, que en materia de protección y seguridad de datos personales se convierten en un reto, el sensibilizar y generar cultura frente al tratamiento de los datos.

Foto: Jorge Jesús - *Pexels*

Con esta estrategia puesta en marcha el desafío fue consolidar el sistema de gestión de la protección de los datos personales administrado por el Oficial. Desafío que comienza con la revisión del estado actual del sistema, actualización a la política de tratamiento de datos, identificación 360 de las bases de datos personales junto con la clasificación de los datos administrados, construcción de un inventario de las bases y, posteriormente, el registro de las bases de datos personales ante la SIC.

Para continuar con la estrategia, en el año 2019 se construyeron cuatro pilares, los cuales fueron fundamentales para dar cobertura al principio de responsabilidad demostrada y evolucionar hacia un sistema de gestión de la seguridad y privacidad de los datos y la información.

En el primer pilar se aborda la **evaluación de impacto en la protección de los datos personales.** La identificación de las amenazas y vulnerabilidades en la gestión de los datos, permitió de forma anticipada identificar la probabilidad y el impacto de la materialización de potenciales riesgos. Para lograr esto, fue fundamental en las mesas de trabajo, explorar el ciclo de vida del dato en relación con las actividades de enseñanza, investigación y extensión. Los líderes de estos temas se convirtieron en aliados estratégicos y bajo su juicio experto, se enfrentaron a repensar escenarios, en los que pueden presentarse eventos de riesgo, que puedan impactar los principios rectores de la ley de protección de datos. Con el resultado del ejercicio, se logró clasificar el nivel de riesgo y la Universidad diseñó y ejecutó planes de acción que permitieron disminuir tanto la probabilidad como el impacto bien sea fortaleciendo controles tecnológicos, de procesos y personas ya implementados o identificando nuevos controles para disminuir el nivel de riesgo. Todo lo anterior se articuló con el sistema de administración de riesgos institucional.

En este orden de ideas, para el año 2019, la Universidad contaba con el "Mapa de riesgos en protección de datos personales" resultado de la identificación, análisis y valoración detallada, como una herramienta clave que permitió dimensionar los eventos que podían materializarse y su magnitud, estableciendo así un *roadmap* para la generación de estrategias con los riesgos de mayor criticidad. En el año 2020, con la presentación de un evento desconocido en el mundo, como fue la pandemia (COVID 19), el desafío fue aun mayor, ya que para la prestación del servicio de educación superior se tuvo que realizar ajustes principalmente en la forma de dictar clase y en servicios que se prestaban de forma presencial, pasarlos a forma virtual. Esto implicó la revisión e inclusión de nuevas finalidades para el tratamiento de los datos, ajustes en las autorizaciones, revisión de las modalidades en la forma de capturar los datos, entre otros retos a los cuales la mayoría de las instituciones de educación se enfrentaron.

En ese mismo sentido, y como efecto de la pandemia, fue realizada una campaña dirigida a los estudiantes frente a la protección de datos en lo relacionado con las grabaciones de la voz e imagen y que siendo datos sensibles, se requirió ampliar la finalidad del tratamiento de datos personales. Lo anterior requirió que los estudiantes leyeran, entendiera y otorgaran nuevamente la autorización del tratamiento de los datos a la Universidad, y esto hizo parte del cambio que se vivió en las clases virtuales y con la metodología *hyflex*.

En definitiva, esta herramienta no solo permitió tener la identificación, clasificación y valoración de los riesgos en la gestión de datos, sino que contribuyó a que desde la planeación estratégica se diseñaran alertas e instrumentos para la disminución del riesgo frente a la parte económica, reputacional, legal y operativa. Del mismo modo, con cierta periodicidad se realizan auditorías al sistema de administración de riesgos para evaluar el nivel de madurez.

Llegados a este punto, el segundo pilar fue establecer, como proyecto estratégico, **la gestión de los activos de información**. En el año 2021, se planteó e inició el desarrollo del proyecto a través de unas etapas, las cuales integraron a todas las áreas de la Universidad. Iniciando con la identificación y valoración de la información clave que es gestionada en los procesos críticos de la Universidad, administrada por las diferentes áreas y a su vez haciendo

especial énfasis en las bases de datos personales. Cabe agregar que el punto de partida inicia con la adopción de normas, guías, estándares que ya existen en el mercado y que fueron adaptadas con base en las necesidades de la Universidad.

Con la ejecución del proyecto, en la primera etapa se consolida una versión uno, con la información de los activos pertenecientes a los procesos críticos, permitiendo analizar, clasificar y valorar los datos personales y la información. Esto con el fin de disminuir la probabilidad de riesgo y los impactos asociados a la seguridad de la información, evitando pérdidas financieras, reputacionales, legales y operativas. En consecuencia, esto asegura el cumplimiento de los requisitos comerciales, legales, contractuales y reglamentarios, asegura la integridad, disponibilidad y confidencialidad de los datos y la información, y aplica buenas prácticas reconocidas y acreditadas de seguridad de la información y protección de datos personales.

Durante el año 2022 se toma como línea base, la curva de aprendizaje y las lecciones aprendidas de la etapa uno. Incluso, el contar nuevamente con la participación de algunos líderes de la etapa uno, permitió la fácil ejecución del proyecto y la generación de conocimiento respecto de los activos de información. Con la segunda etapa se da cobertura a los procesos que hacen parte del sistema de gestión de calidad de la Universidad. Al finalizar, se obtiene el logro de contar con la identificación, clasificación y valoración de los activos, con un nivel de detalle respecto a la clasificación de los datos personales (sensible, privado, semiprivado, público) y la información (pública, restringida, confidencial).

De esta manera, la unión del mundo de la protección de los datos personales y la seguridad de la información han contribuido al fortalecimiento del sistema de gestión de la seguridad y privacidad de los datos y la información.

Lo anterior significa que, herramientas como la "matriz de activos de información" y el "mapa de riesgos", permiten tener información a la mano, lo cual es fundamental para la toma de decisiones.

Siguiendo con la estrategia, se formuló el tercer pilar **evaluación, control y mejora.** En el marco del sistema de gestión de la seguridad y privacidad de los datos y la información, es preciso mencionar que se ejecutaron auditorías, que permitieron identificar potenciales puntos de fallo, lo cual llevó a ejecutar acciones tempranas para disminuir la materialización de un riesgo. Durante el año, los diferentes procesos del sistema de gestión de calidad, son auditados teniendo en cuenta la protección de los datos personales.

Con los informes de auditoría, se implementan planes de acción o se busca el fortalecimiento en los procesos que apalancan la estrategia en protección y seguridad de los datos personales y la información. En otro aspecto, la gestión de incidentes hace parte vital de este pilar. Ante cualquier señal de alarma o ante el anuncio de un potencial incidente de seguridad en los datos, se activa el protocolo. Con ocasión de dar un mayor entendimiento a los miembros del comité estratégico en protección de datos de cualquier incidente, el oficial construye un informe para presentar los hechos, de tal forma que reconstruye el caso a través de una línea

de tiempo. Una explicación que permite identificar todos los actores y sistemas de información intervinientes, contemplando uso de palabras de fácil entendimiento.

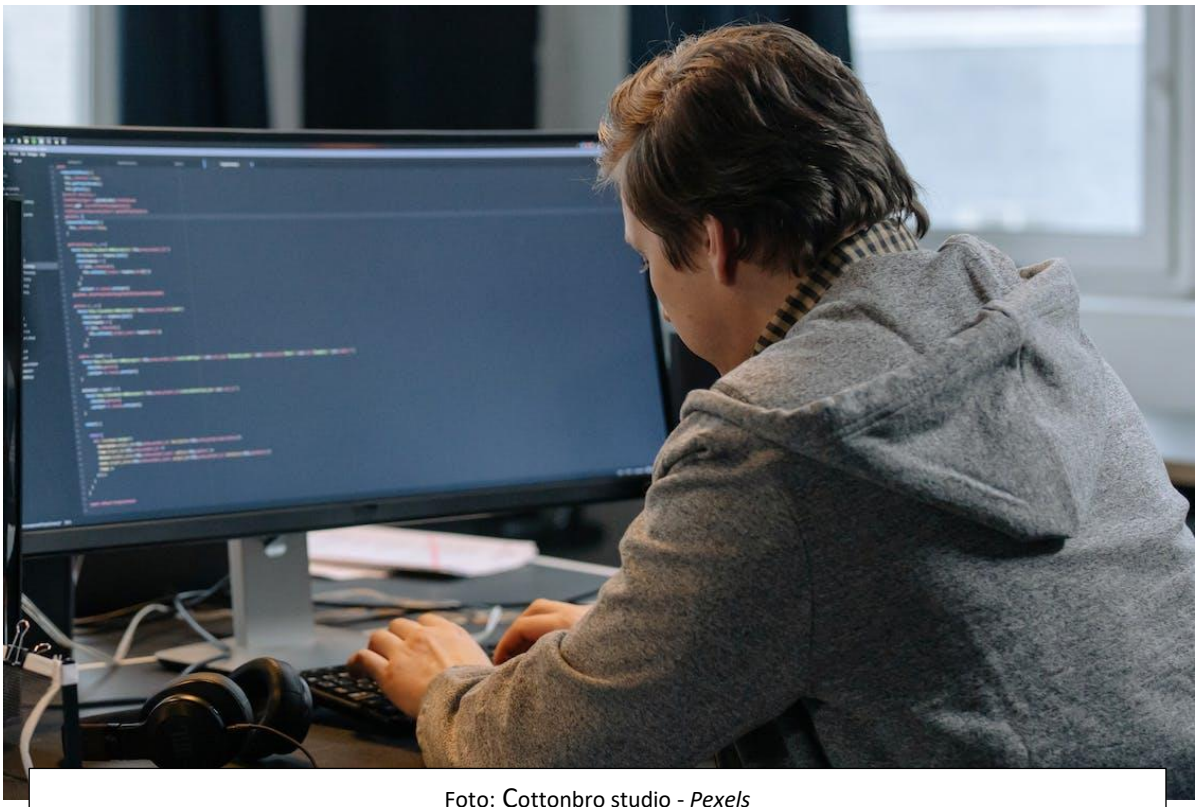

Foto: Cottonbro studio - *Pexels*

Para el Oficial de Seguridad de la Información y Datos Personales, el liderar la presentación y relato de los hechos, implicó hacer una propuesta de *storytelling* como técnica de comunicación que de manera efectiva y enfocada en la línea de tiempo que soporta los hechos, se articuló con el esquema de trabajo que desde las metodologías de planeación estratégica se realizan en la Universidad, y permitió que el informe diera una nueva connotación a la toma de decisiones del comité.

En ese contexto, y con los resultados de los tres pilares anteriores, fue necesario trascender en la apropiación y concientización a todos los niveles de cargos dentro de la Universidad. Uno de los temas más desafiantes fue lograr que las personas interiorizaran y apropiaran el tema de protección de datos personales y seguridad de la información. Por esto, la cultura de la protección de datos personales requirió de campañas pedagógicas, de fácil entendimiento y que llegaran a todas las audiencias, dando paso al cuarto pilar: **cultura en datos personales y seguridad de la información**. El acercamiento en jornadas de planeación donde participan todos los directivos, los decanos(as) y vicedecanos(as), profesores, estudiantes y empleados, bajo el desarrollo de talleres, cursos, infografías, capacitaciones, diseñados para generar un ambiente amigable y cercano al público han permitido innovar en las estrategias de comunicación. Generar sensibilización frente a

lineamientos en el tratamiento de los datos, la importancia de reconocer el buen uso y manejo de los datos personales, los riesgos a los cuales se exponen potencialmente las personas frente a un descuido o mal manejo de los datos, el cuidado al manejar datos de tipo sensible y de menores de edad, entre otros temas, han sido la bandera del Oficial para atraer más personas al mundo de la protección de los datos personales. Seguido a esto, en la cultura de gestión de datos fue clave no permanecer estáticos, en especial con la recopilación y tratamiento de datos personales de menores de edad, la capacitación al equipo de la dirección de marketing y al equipo UR Partner, integrado por estudiantes que apoyan en las actividades de promoción y atracción de estudiantes ha sido fundamental para fortalecer la apropiación y sensibilización de las finalidades del tratamiento de datos y evitar que se presente un inadecuado manejo.

Si bien se implementaron capacitaciones continuas en la Comunidad Rosarista frente a la protección de los datos personales desde la publicación de la ley, es en el año 2019 donde, a través de una alianza con la SIC, se impulsó a los empleados a realizar el curso en protección de datos personales. Más de 700 participantes fueron certificados en un conocimiento básico en la protección de los datos. Entre los años 2020 y 2022 se ha avanzado complementando la estrategia del uso de plataforma de la SIC, con una plataforma de uso interno, logrando más de 560 empleados. Desde el año 2022 la Dirección Académica ha validado para los profesores, como curso de desarrollo profesoral, el curso en protección de datos personales y el curso de ciberseguridad, dada la acogida y la importancia en la apropiación por parte del equipo profesoral.

Así, considerar la gestión de datos personales y seguridad de la información como parte de la planeación estratégica de la Universidad ha sido clave para la solidez del sistema de gestión de la seguridad y privacidad de los datos y la información. La consolidación de los cuatro pilares, que han permitido tener el mapa de riesgos de datos personales, la matriz de activos de información, el fortalecimiento del monitoreo, evaluación y gestión de incidentes, así como el impulso en la sensibilización y cultura de la gestión de datos personales convergen en la mirada integral donde se tiene en cuenta la visión 360 del dato, su ciclo de vida, su tratamiento desde lo jurídico, tecnológico, de procesos, de seguridad y privacidad.

Con todo lo anterior, es preciso resumir que el compromiso de todos los actores que integran el sistema de gestión de la seguridad y privacidad de los datos y la información han sido claves para el desarrollo, constitución y fortalecimiento del mismo.