UNIVERSIDAD NACIONAL DE MAR DEL PLATA

FACULTAD DE HUMANIDADES

DEPARTAMENTO DE CIENCIA DE LA INFORMACIÓN

EDUCACIÓN A DISTANCIA

LICENCIATURA EN BIBLIOTECOLOGÍA Y DOCUMENTACIÓN

(LICAD)

TESINA

Ley 25.326/00 de Hábeas Data. Estrategias para la protección de datos personales en bibliotecas universitarias públicas y privadas de la República Argentina. Un estudio exploratorio descriptivo

Autora: Camila Ludueña
Director: Ab. Sergio Aguirre
Co Directora: Lic. Laura Daniela Orellano
Título a obtener: Licenciatura en Bibliotecología y Documentación
Lugar y fecha: Córdoba, Provincia de Córdoba, 2024

Resumen

En la presente tesina se da respuesta al problema de investigación que corresponde a la siguiente pregunta: ¿Qué estrategias implementan las bibliotecas universitarias públicas y privadas de la República Argentina para proteger los datos personales de los usuarios garantizando la aplicación de la Ley de Hábeas Data vigente? Al analizar esta legislación, como marco normativo para la protección de datos personales, queda claramente establecida su relevancia. Luego de efectuar un recorrido por las diferentes normas que rigen el tratamiento de datos personales en las bibliotecas universitarias públicas y privadas argentinas, se encuentra que, ninguna de ellas posee un documento propio, destinado a regular integralmente los procedimientos que involucran el manejo de información personal. En general, cada una adhiere a la política de privacidad de la universidad a la que pertenece. Esta ausencia implicó la necesidad de indagar en la normativa sobre el tema a nivel internacional. Para profundizar, se analizan los casos de Estados Unidos, México y España en relación a sus disposiciones sobre protección de datos personales y su aplicación en el entorno bibliotecario. Por otra parte, de acuerdo a la encuesta realizada para esta investigación sobre estrategias de implementación de la Ley de Hábeas Data en bibliotecas universitarias argentinas, los resultados confirman las ausencias mencionadas en el tratamiento y protección de datos personales. Si bien no existen “recetas” para ser adoptadas por todas las bibliotecas, en un contexto digitalizado y complejo como el actual, los datos que manejan exigen el diseño de un instrumento propio para la aplicación de métodos de protección de información personal. Frente a esto, se desarrolla una lista de sugerencias como un aporte significativo desde esta investigación.

Palabras clave: Ley 25.326/00 de Hábeas Data, protección de datos personales, marcos normativos y protocolos internacionales, políticas de privacidad en bibliotecas públicas y privadas, estrategias de implementación.

Abstract

This thesis addresses the research question: What strategies do public and private university libraries in Argentina implement to protect users' personal data, ensuring the application of the current Data Protection Law? Through an analysis of this legislation as a regulatory framework for personal data protection, its relevance is clearly established. A review of the different regulations governing personal data handling in Argentine public and private university libraries reveals that none have their own specific document comprehensively regulating procedures involving personal information management. Instead, most libraries follow the privacy policy of their parent university. This lack of specific guidelines prompted an exploration of relevant international standards. To deepen the analysis, cases from the United States, Mexico, and Spain are examined regarding their personal data protection regulations and their application in the library environment. Additionally, results from a survey conducted for this research on the implementation strategies of the Data Protection Law in Argentine university libraries confirm the previously mentioned gaps in data handling and protection practices. While there are no universal "recipes" that can be adopted by all libraries, in a complex, digitized environment such as today’s, the data they manage requires designing a specific instrument for applying personal data protection methods. Accordingly, this research proposes a set of recommendations as a significant contribution.

Keywords: Law 25.326/00 on Habeas Data, protection of personal data, regulatory frameworks and international protocols, privacy policies in public and private libraries, implementation strategies.

Índice

Introducción..... 7

Estado del Arte..... 10

Capítulo 1: Ley 25.326 Hábeas Data. Protección de los Datos Personales..... 14

1.1. Disposiciones y principios generales relativos a la protección de datos..... 14

1.1.1. Tipos de datos personales. Bancos y bases de datos comprendidos. Titulares y usuarios de datos..... 15

1.1.2. Consentimiento e información..... 17

1.1.3. Calidad y cesión de datos..... 18

1.2. Derechos de los titulares de datos..... 20

1.2.1. De información, acceso y contenido..... 20

1.2.2. Derecho de rectificación, actualización o supresión..... 20

1.3. Archivos, registros, bases o bancos de datos. Usuarios y responsables..... 21

1.3.1. Formación de archivos, registros, bases o bancos de datos..... 21

1.3.2. Deberes de los responsables..... 22

1.3.3. Contrato de servicios informatizados de datos personales..... 24

Capítulo 2: Normativa sobre protección de datos personales en el ámbito internacional. Los casos de América del Norte y Europa. Impacto sobre las bibliotecas de Estados Unidos, México y España..... 26

2.1. Organismos supranacionales. Protección de Datos Personales en bibliotecas..... 26

2.2. La Protección de Datos Personales en Estados Unidos..... 31

2.2.1. Asociación de Bibliotecas de Estados Unidos..... 33

2.3. La Protección de Datos Personales en México..... 37

2.3.1. Colegio Nacional de Bibliotecarios de México..... 41

2.4. La Protección de Datos Personales en España..... 42

2.4.1. Federación Española de Sociedades de Archivística, Biblioteconomía, Documentación y Museística..... 44

Capítulo 3: Las políticas y estrategias implementadas en las bibliotecas universitarias públicas y privadas relevadas de América y Europa..... 47

3.1. Políticas y estrategias de protección de datos personales de usuarios de bibliotecas. Contextualización y criterios de selección de las bibliotecas públicas y privadas de América y Europa..... 47
3.2. Estados Unidos..... 48
3.2.1. Biblioteca Digital de la Universidad de California (pública).....48
3.2.2. Biblioteca del Instituto Tecnológico de Massachusetts (privada).....52
3.3. México..... 57
3.3.1. Biblioteca Central de la Universidad Nacional Autónoma de México (pública)..... 57
3.3.2. Biblioteca de la Universidad La Salle (privada).....62
3.4. España..... 63
3.4.1. Biblioteca de la Universidad de Cantabria (pública)..... 63
3.4.2. Biblioteca de la Universidad Alfonso X el Sabio (privada)..... 66
Capítulo 4: Presentación y análisis de los datos..... 72
4.1. Metodología implementada..... 72
4.2. Relevamiento y presentación de los datos.....77
4.3. Respuestas obtenidas..... 77
4.3.1. Dimensión Normativa.....77
4.3.2. Dimensión Datos.....79
4.3.3. Dimensión Usuarios..... 84
4.3.4. Dimensión SIGB y servicios web..... 86
4.3.5. Dimensión formación de usuarios y del personal bibliotecario..... 90
4.4. Interpretación de los datos..... 91
Conclusiones..... 100
Referencias bibliográficas.....107
Anexo..... 117

Índice de tablas

Tabla 1: Provincias, universidades nacionales y bibliotecas argentinas. 77

Tabla 2: Provincias, universidades privadas y bibliotecas argentinas. 78

Tabla 3: Dimensiones y variables. 79

Introducción

En el año 2000, en la República Argentina, se sanciona la Ley 25.326 de Protección de los Datos Personales, conocida como Ley de Hábeas Data. Esta legislación contempla la protección y resguardo de la información personal registrada en archivos o bancos de datos, sean estos públicos o privados. Así, se busca garantizar el derecho de los individuos sobre el conjunto de datos vinculados a su honor e intimidad.

Entendiendo que esta ley es el marco para la recolección, tratamiento y uso de los datos personales, las bibliotecas universitarias públicas y privadas no están exentas de la aplicación de dicha norma, considerando que sus usuarios ponen a su disposición información personal que circula por diferentes plataformas y redes.

La regulación sobre la protección de datos personales -PDP- es cada día una demanda más acuciante, si se tiene en cuenta el nivel de injerencia de los avances tecnológicos. En el contexto de las bibliotecas universitarias, la mayoría de ellas carece de políticas de protección propias, disponibles de manera accesible en sus sitios web oficiales. Sin embargo, es importante considerar que no todos los procedimientos y servicios bibliotecarios pueden reflejarse completamente en una plataforma en línea, lo cual subraya la necesidad de un análisis más profundo sobre las acciones implementadas en la práctica cotidiana.

En general, el aviso de privacidad de la universidad en el marco de la cual operan, es el único espacio donde el público puede informarse sobre cómo se recogen, tratan y utilizan los datos proporcionados a las unidades de información. Asimismo, es fundamental destacar que, si entre las estrategias adoptadas no se cuenta con una formación para los usuarios en el ejercicio de sus propios derechos, es poco probable que se tenga conocimiento de cuáles son y cómo deben aplicarlos. En este sentido, tanto el rol de las bibliotecas, como el de su personal se torna relevante, dado que, desde su accionar, pueden contribuir a la institucionalización de las leyes de protección de datos personales, para que las personas reconozcan y gestionen con mayor autonomía el uso de su información.

Por lo tanto, la PDP sigue siendo una asignatura pendiente en muchas bibliotecas universitarias argentinas, ya que se detectan ausencias y falta de

especificidad respecto al tratamiento de la información personal de sus usuarios. Tanto la recopilación, como el almacenamiento de estos datos conlleva riesgos, y si no se implementan las medidas de seguridad y transparencia necesarias para garantizar la privacidad, el marco normativo en vigor no se cumple plenamente.

Cuando se recorre la bibliografía disponible a nivel internacional, se observan enfoques diversos sobre esta temática. Además, se encuentran políticas de privacidad elaboradas por bibliotecas académicas, tanto de Europa como de América, que desde hace al menos una década consideran a la protección de los datos personales de los usuarios como un aspecto fundamental en la prestación de sus servicios. No obstante, no es esta la realidad que se observa en la República Argentina.

Por lo expresado, el problema de investigación se plantea de la siguiente manera: ¿qué estrategias implementan las bibliotecas universitarias públicas y privadas de la República Argentina para proteger los datos personales de los usuarios garantizando la aplicación de la Ley de Hábeas Data vigente?

Esta problemática aborda como objetivo general: analizar las estrategias que implementan las bibliotecas universitarias públicas y privadas de la República Argentina para proteger los datos personales de sus usuarios, garantizando la aplicación de la Ley de Hábeas Data vigente. Y se operacionaliza en los siguientes objetivos particulares: evaluar reglamentos y políticas de privacidad de bibliotecas universitarias públicas y privadas argentinas, para determinar en qué medida estos incluyen acciones orientadas a garantizar el cumplimiento de la Ley 25.326/00; describir el tipo de datos personales solicitados por bibliotecas universitarias públicas y privadas argentinas a sus usuarios, y el tratamiento de los mismos a la hora de brindar servicios web; relevar la capacitación del personal bibliotecario respecto a estrategias para la protección de datos personales; comparar el tratamiento y protección de datos personales de usuarios entre bibliotecas universitarias públicas y privadas; desarrollar sugerencias para optimizar las prácticas de protección de datos personales en bibliotecas universitarias.

De esta manera, la presente tesina se estructura como sigue: en el capítulo 1, se desarrolla un análisis acerca de la Ley 25.326 de Protección de los Datos Personales, como marco legal vigente en la República Argentina; en el capítulo 2, se

aborda la normativa internacional sobre protección de datos personales, en particular, los casos de Estados Unidos, México y España; en el capítulo 3, se describen las políticas de protección de datos de usuarios derivadas de las disposiciones analizadas previamente, elaboradas por unidades de información públicas y privadas de los países mencionados; en el capítulo 4, se presenta la metodología implementada, el relevamiento y presentación de los datos recopilados a través de la encuesta realizada a bibliotecas universitarias argentinas públicas y privadas, y su interpretación. Posteriormente se arriba a las Conclusiones, a partir de las cuales se desarrolla una lista de sugerencias para la protección de datos personales en bibliotecas universitarias, según la legislación nacional vigente.

Estado del Arte

El presente estudio se enfoca en la aplicación de la Ley 25.326/00 de Protección de los Datos Personales en bibliotecas universitarias públicas y privadas de la República Argentina. Para ello, en primera instancia, se realiza un relevamiento de los sitios web de 49 unidades de información universitarias[1], localizadas en las 23 provincias argentinas y la Ciudad Autónoma de Buenos Aires.

A partir de este procedimiento, se advierte que 44 de las sedes web de las unidades de información verificadas no mencionan las condiciones de privacidad de los usuarios que acceden a sus servicios. Solo 2 bibliotecas universitarias públicas y 1 privada[2] hacen una breve referencia, en distintos documentos oficiales, a la garantía de confidencialidad en el tratamiento de los datos personales.

Las únicas bibliotecas universitarias que mencionan de manera explícita la Ley de Hábeas Data son, en primer lugar, la perteneciente a la Universidad Nacional de San Luis (2021), que en el Artículo 13 de su reglamento, establece que “el Sistema de Bibliotecas se compromete a mantener la confidencialidad de los datos de los usuarios y sus transacciones conforme a la legislación vigente” (p. 10). En tanto, el Sistema de Bibliotecas de la Universidad Católica de Córdoba (2024), manifiesta a través de sus “Políticas de comunicación”, que los datos personales de sus usuarios:

> Serán utilizados con el único propósito de atender sus peticiones, serán almacenados y resguardados en el UCCb, y no serán proporcionados a terceros. El UCCb se rige en lo referente a la protección de datos personales por lo previsto en la Ley 25.326. (p.4)

Además, se considera pertinente señalar que no fue posible recuperar normas de asociaciones representantes de bibliotecas y bibliotecarios en donde se haga

[1]Listado disponible en el Anexo.
[2]Biblioteca Pública de la Universidad Nacional de La Plata: https://www.biblio.unlp.edu.ar/institucional/pautas-de-convivencia-14669; Sistema de Bibliotecas y Gestión del Conocimiento de la Universidad Nacional de Tierra del Fuego, Antártida e Islas del Atlántico Sur: https://untdf.edu.ar/institucional/secretarias/secretaria_academica/sistema_de_bibliotecas_y_gestion_del_conocimiento; Universidad de Belgrano: https://biblioteca.ub.edu.ar/cgi-bin/koha/pages.pl?p=reg.

referencia a la ética profesional en el manejo de datos personales de usuarios. Sin embargo, se observan ciertos “esfuerzos como el Anteproyecto del Código de Ética del Profesional Bibliotecario de Córdoba, el Código de Ética de ABDAM, de Mar del Plata, y algunos intentos en Buenos Aires y San Juan” (Kraemer, 2011, p. 9). Así como también, el Proyecto de Ley para un Estatuto del Profesional en Bibliotecología y Documentación para la Argentina presentado a la Cámara de Diputados de la Nación en el año 2005 y caducado en 2007[3].

De la misma manera, no se encontraron antecedentes nacionales de estudios o investigaciones que aborden las estrategias aplicadas por las bibliotecas universitarias para garantizar el cumplimiento de la Ley 25.326 de Protección de los Datos Personales. No obstante, se rescatan una serie de recomendaciones desarrolladas por Reggiani (2006) para todo tipo de unidades de información, las cuales consisten en: reforzar medidas para garantizar la privacidad de los registros de los usuarios, el deber de alertarlos acerca de las posibles filtraciones que escapan al control de la biblioteca y determinar las actividades que están sujetas o no a la protección del secreto profesional.

Frente a este panorama, se recurre a la revisión de literatura internacional. En principio, se toma como antecedente central el estudio realizado por Varela-Orol y Ameneiros Rodríguez (2018), el cual releva la disponibilidad de políticas de privacidad en las sedes web de bibliotecas universitarias de España. Dicho trabajo se centra en 49 bibliotecas de universidades públicas y tiene como marco legal el Reglamento General de Protección de Datos de la Unión Europea. Los temas analizados giran en torno a la información proporcionada a los usuarios respecto al registro, tratamiento y protección de sus datos personales; seguridad de las sedes web y catálogos en línea; formación de usuarios en cuanto a la protección de su información personal en el ámbito digital; y datos personales en registros bibliográficos.

También se destaca el trabajo de Vaughan (2020), cuyo objetivo es analizar y detallar los principales componentes de políticas de privacidad publicadas por 100

[3] Proyecto de Ley sobre Reglamentación del Ejercicio Profesional en Bibliotecología y Documentación. (2005). https://www.senado.gob.ar/web/proyectos/verExpe.php?origen=S&numexp=799/05&tipo=PL&tConsulta=1

bibliotecas universitarias estadounidenses en sus plataformas en línea. Para la obtención de esta muestra se relevaron 314 sedes web de bibliotecas, detectándose que la mayoría de las unidades de información no cuentan con una política de privacidad propia. Sin embargo, esto no implica que en esos casos no existan estrategias para proteger los datos personales de los usuarios, sino que es posible que éstas no se hagan públicas o que las instituciones se adhieran a las políticas generales de privacidad emitidas por la casa de estudios a la que pertenecen.

A partir de la muestra anteriormente mencionada, Vaughan (2020) señala y analiza los ejes que estructuran los documentos destinados a gestionar la información personal de los usuarios. Estos incluyen: el tipo de datos recopilados y los sistemas que intervienen en su registro; procesamiento y utilidad de los datos; acuerdos con terceros; seguridad, integridad y retención de datos; referencias a leyes, declaraciones de organismos supranacionales, códigos de ética de asociaciones de bibliotecarios, políticas de la institución educativa en la que se enmarcan, procedimientos frente a problemas de seguridad y posible divulgación de datos personales.

Por último, Vega (2022) desarrolla un estudio presentado en tres momentos, sobre el uso de los datos personales en las bibliotecas de México. En el último de estos artículos, la autora se pregunta si es necesario solicitar el consentimiento informado de los usuarios para brindar servicios y realizar estadísticas. A fin de responder a esta cuestión, examina la legislación mexicana en materia de protección de datos personales y destaca los principios fundamentales de estas normativas: licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad. A partir de este análisis, concluye que la aplicación de dichos lineamientos debe ajustarse al propósito específico de uso de los datos, permitiendo así determinar cuándo es necesario obtener el consentimiento explícito o implícito de los titulares.

Aunque los artículos previamente citados como antecedentes para este trabajo de investigación provienen de contextos diferentes, amplían la visión y proporcionan una base para comprender las técnicas implementadas por unidades de información para la protección de datos personales.

Considerando la ausencia de trabajos académicos argentinos en este campo, así como también de políticas de privacidad publicadas en los sitios web de bibliotecas universitarias argentinas públicas y privadas, la presente investigación busca explorar las estrategias de protección de datos personales que, a pesar de no estar reflejadas en línea, podrían ser desarrolladas en la práctica cotidiana de estas unidades de información.

Capítulo 1: Ley 25.326 Hábeas Data. Protección de los Datos Personales

1.1. Disposiciones y principios generales relativos a la protección de datos

La Ley 25.326 de Protección de los Datos Personales, promulgada en el año 2000, regula el *hábeas data*[4] y desde su artículo 1° establece que tiene como objetivo:

> La protección integral de los datos personales asentados en archivos, registros, bancos de datos, (...) sean estos públicos o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre (p.1).

De esta manera, se determina que las garantías expresadas en esta legislación apuntan a proteger la intimidad y el derecho de las personas al acceso a su información personal, alojada en bases datos públicas o privadas. Según Basterra (2010), la intimidad es un derecho fundamental que se entiende como el ámbito de la vida de un individuo que no está destinado a ser conocido por otros e implica la facultad de las personas para decidir qué datos de sí se mantienen en privado. Este derecho se percibe bajo riesgo por el avance de las tecnologías y servicios que requieren proporcionar información personal, la cual es almacenada en archivos o bancos de datos, y puede ser objeto de uso indebido.

Frente a esto, la Protección de Datos Personales -en adelante PDP- surge como un "conjunto de medidas para garantizar y proteger los datos de carácter personal (...) que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado" (Diccionario panhispánico del español jurídico, 2023, párr. 1). Es decir, son medidas destinadas a garantizar la privacidad de los datos de carácter personal, la seguridad de su almacenamiento, regular su transmisión y tratamiento en todos los ámbitos.

[4] "El enunciado hábeas data se forma con hábeas, que proviene del latín *habeo, habere* que significa tener, exhibir, tomar, traer, etc.; adosándole el término data, respecto del cual existe alguna disputa léxica. Mientras algunos autores afirman que se refiere al acusativo neutro plural de *datum*; lo que se da -datos- también del latín; para otros, el vocablo es de origen inglés y hace referencia a información o datos; en el caso, la traducción sería "tienes tus datos" (Basterra, 2010, p. 1).

Se considera que la protección de datos personales es un derecho fundamental contemplado a nivel internacional por el artículo 12 de la Declaración Universal de Derechos Humanos[5], así como a nivel local por el artículo 43, párrafo tercero, de la Constitución nacional[6] y, con mayor profundidad, mediante la Ley 25.326. Estos marcos legales establecen los cimientos sobre los que todo organismo que trabaja con datos personales debe diseñar sus prestaciones. Tal es el caso de las bibliotecas, las cuales, de acuerdo con Varela-Orol y Ameneiros Rodríguez (2018), siempre les han solicitado a sus usuarios múltiples datos personales a fin de prestar sus servicios.

Para continuar con el desarrollo de este capítulo se procede a recorrer los artículos de la Ley 25.326 que se consideran significativos para este estudio, así como a señalar el alcance de esta legislación sobre el ámbito de las bibliotecas.

1.1.1. Tipos de datos personales. Bancos y bases de datos comprendidos. Titulares y usuarios de datos

El artículo 2 de la Ley 25.326 de Protección de los Datos Personales de 2000, tiene como objetivo brindar definiciones que aportan claridad respecto a los conceptos regulados por la normativa y reducir “los conflictos derivados de la interpretación de los términos o conceptos utilizados en la ley" (Ramos, 2007, p. 8). Con este propósito, el artículo proporciona una clasificación de los diferentes tipos de datos, su tratamiento, define qué son los archivos, registros, bases o bancos de datos y especifica quiénes son los titulares de los datos, así como también los usuarios.

En primer lugar, se describe a los datos personales como todo tipo de información referida a personas físicas o no; mientras que los datos sensibles son

[5] Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques (Asamblea General de las Naciones Unidas, 1948, artículo 12).

[6] Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística (Constitución de la Nación Argentina, 1994, artículo 43).

categorizados como aquellos que revelan origen racial y étnico, opiniones políticas, creencias religiosas, filosóficas o morales, afiliación sindical, estado de salud e información sobre la sexualidad de un individuo. Además, se estipula que los datos informatizados son aquellos que han sido procesados electrónicamente o automatizados.

Por tanto, la definición de datos personales establecida en la Ley 25.326 es sumamente amplia, puesto que engloba toda aquella información que permita identificar de manera directa o indirecta a una persona. Además, según Basterra (2010), dicha capacidad de identificación es la razón fundamental detrás de la protección de los datos personales, pues a través de ellos se puede reconocer tanto la identidad de un individuo, como señalar sus conductas y prácticas habituales.

Respecto a los datos sensibles, se comprende que abarcan los datos vinculados con las ideologías políticas y religiosas de una persona, así como su origen étnico y orientación sexual. Estos últimos son particularmente confidenciales ya que, según Ramos (2007), pueden afectar su intimidad y vinculados con un dato personal, pueden llevar a describir el perfil completo de un individuo.

En cuanto a la información personal que las bibliotecas pueden solicitar y almacenar de sus usuarios, está es variada y depende de los requisitos de cada unidad de información para brindar acceso a sus servicios. En este ámbito, es importante destacar la discusión planteada por Lencinas (2004), quién señala que, si bien el registro o historial de las consultas bibliográficas realizadas por los usuarios no se considerada como dato "sensible" según la definición legal, al combinarlos o cruzarlos con la información personal registrada en la biblioteca, es posible obtener información que permita crear perfiles ideológicos de los usuarios. De la misma manera, Reggiani (2006) sostiene que este tipo de información debe considerarse como datos sensibles. Por lo tanto, se considera que este tipo de datos deben ser cuidadosamente observados y protegidos en las bibliotecas, así como toda la información sobre el uso que el público hace de los servicios de las unidades de información.

Por otra parte, el artículo 2 de la Ley 25.326, establece que los archivos, registros, bases o banco de datos están conformados por un conjunto de datos personales, que reciben un procesamiento -electrónico o no-, cualquiera sea su

organización y acceso. Además, se designa a los titulares de archivos, registros, bases o banco de datos, como sus responsables.

En cuanto a los titulares de los datos, la legislación los define como toda persona cuyos datos personales sean tratados y procesados por archivos o bancos de datos. Mientras que los usuarios, son toda persona, pública o privada, que ejerza el procesamiento de esta información en archivos, registros, bases o bancos de datos.

Por lo tanto, al aplicar lo establecido por la Ley 25.326 en el contexto de las transacciones habituales que ocurren en una biblioteca, se puede inferir que los usuarios son los titulares de los datos, ya que deben proporcionar información personal para acceder a ciertos servicios de la unidad de información. La biblioteca, como entidad titular de las bases de datos utilizadas para ofrecer prestaciones, es la responsable de la gestión de los datos. En tanto, los profesionales de la información son los usuarios, ya que se encargan de registrarlos y llevar a cabo su procesamiento.

1.1.2. Consentimiento e información

En el artículo 5 de la mencionada Ley se determina que “el tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias”. (p.3)

Por lo tanto, puede inferirse que toda biblioteca que solicite información personal a sus usuarios debe informar sobre el tratamiento de los datos personales y obtener el consentimiento para su procesamiento. En relación a esto, Basterra (2004) sostiene que la forma más sólida de registrar el consentimiento del titular es mediante la firma escrita del documento que contiene la información sobre el procesamiento de los datos o del formulario utilizado para recopilar dicha información.

Además, en el artículo 6, se especifica que al momento de recoger sus datos personales, se deberá notificar a los titulares: la finalidad del tratamiento que se le dará a la información proporcionada y sus destinatarios; el archivo, registro o banco de datos donde serán almacenados, así como también la identidad y domicilio de su

responsable; el carácter obligatorio o facultativo de las respuestas que deberá dar para el cuestionario de recolección de datos; las consecuencias derivadas de aportar o no sus datos, ya sea de manera inexacta o incompleta; los derechos como titular a acceder, rectificar y suprimir sus datos.

No obstante, es importante destacar que, según versa la Ley 25.326, sólo en determinados casos, el consentimiento no será necesario, a saber: los datos puedan ser obtenidos de fuentes de acceso libre y público; deban ser recabados por una obligación legal o los datos requeridos se limiten a: nombre, documento nacional de identidad, identificación tributaria, ocupación, fecha de nacimiento y domicilio.

1.1.3. Calidad y cesión de datos

Para desarrollar este apartado, es necesario mencionar lo establecido por el artículo 4 de la Ley 25.326. Dicho artículo se refiere a la calidad que deben tener los datos personales recolectados, haciendo especial hincapié en su exactitud, pertinencia con los objetivos del tratamiento que recibirán, accesibilidad, posibilidad de actualización y supresión. Detalla, además, que los datos deben ser destruidos cuando hayan dejado de ser necesarios respecto al propósito por el cual fueron registrados.

Respecto a esto, Basterra (2013) explica que el requerimiento de que la información personal esté actualizada representa, en primer lugar, un derecho del individuo al que pertenecen los datos y, en segundo lugar, una responsabilidad establecida por la ley para los titulares, usuarios o responsables de bancos o archivos.

Estas nociones son de vital importancia para la gestión de datos personales en bibliotecas, ya que su aplicación permite proveer servicios personalizados basados en información precisa y actualizada sobre los usuarios, tal como la Diseminación Selectiva de Información -DSL-. Además, la disposición de eliminar los datos cuando dejan de ser relevantes promueve una gestión responsable de la información personal almacenada sobre el público que accede a una biblioteca. En palabras de Lencinas (2004), prácticas como “almacenar datos sobre préstamos devueltos (el famoso "Historial") es simplemente contrario a la ley de Hábeas Data”

(p.4), por lo que “la eliminación permanente de datos que ya no son necesarios” (p.4) se constituye como una acción necesaria para la PDP.

Más adelante en el texto del artículo 7 de la legislación nacional, se abarca la obtención y tratamiento de datos sensibles en particular. Determinando que a ninguna persona se le puede imponer la obligación de proporcionar este tipo de información y prohíbe la conformación de archivos, bancos o registros que los revelen, directa o indirectamente. Además, se deja asentado que sólo pueden ser recolectados y sometidos a tratamiento frente a razones de interés general autorizadas por la ley. Aclara también que, para uso científico o estadístico, dicha información no puede estar asociada a sus titulares.

Esto toma relevancia en el mundo de las bibliotecas, al tener en cuenta que, de acuerdo con Venteño Jaramillo y Casas Castillo (2013), frecuentemente se aplican técnicas estadísticas para realizar estudios de usuarios y análisis de uso de las colecciones. Lo cual involucra datos tales como registros de préstamos, frecuencia de uso de bases de datos, búsquedas bibliográficas, entre otros. Por lo cual, la anonimización de los datos es un procedimiento fundamental que deben ejecutar las unidades de información.

Además, el artículo 11, establece que los datos personales sólo pueden ser cedidos a terceros a fin de cumplir con el propósito de tratamiento de los datos explicitado por el usuario al titular, quien deberá dar su consentimiento previo y tendrá derecho a revocarlo en caso de considerarlo necesario. Dicha aprobación para la cesión de los datos no es exigida cuando, entre otros casos, la información haya sido disociada de sus titulares. Cabe agregar que el cesionario de los datos está sujeto a las mismas obligaciones legales que el cedente y deberá responder por él ante el organismo de control correspondiente.

Este último punto es aplicable en el ámbito bibliotecario dada la numerosa cantidad de acuerdos con terceros que puede sostener una unidad de información para brindar servicios, tales como los mencionados por Merlo Vega (2005): préstamo interbibliotecario, servicios comerciales para consulta de colecciones electrónicas, suscripciones a publicaciones periódicas, colaboraciones con empresas de tecnología, proveedores de SIGB, entre otros. En función de esto, se torna imprescindible la necesidad de disociar los datos personales de sus titulares o

requerirles consentimiento a los usuarios de la biblioteca para su transferencia y procesamiento por parte de terceros.

1.2. Derechos de los titulares de datos

1.2.1. De información, acceso y contenido

En primer lugar, el artículo 13 de la Ley 25.326, estipula el derecho a la información, manifestando que “toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables” (p.5). Más adelante, en el artículo 14 se describe el derecho al acceso como la facultad que tiene cualquier ciudadano, previa acreditación de su identidad, para solicitar información sobre los datos personales que se tienen sobre él en archivos o bases de datos. Por otra parte, el artículo 15 detalla el contenido del informe que debe proporcionar el usuario de los datos al titular. Se expresa que la información debe ser completa, clara, comprensible y presentada en el soporte que éste último prefiera.

Por lo tanto, estos apartados de la Ley le otorgan a los ciudadanos un mayor control sobre sus datos personales, al regular y garantizar el procedimiento para solicitar la identificación de bases de datos, conocer la información personal que almacenan y recibir un informe claro y completo de parte de los responsables.

Dentro del contexto de las bibliotecas, la legislación vigente ampara el derecho de los usuarios -titulares de datos-, a conocer y controlar su información personal alojada en las bases de datos utilizadas para la gestión de los servicios bibliotecarios. Estas facultades son coherentes con lo expresado por la Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas -IFLA- (2012), que destaca la importancia de apoyar y promover la transparencia en todas las instituciones, para que estén abiertas al escrutinio público.

1.2.2. Derecho de rectificación, actualización o supresión

El artículo 16 de la Ley anteriormente mencionada, se refiere al derecho que tienen los titulares de datos personales a solicitar la corrección, actualización,

confidencialidad o eliminación de la información inexacta, incompleta o desactualizada que se tiene sobre ellos en bases de datos públicas o privadas.

A su vez, el artículo establece que el responsable de un archivo, registro o base de datos debe informar al titular de los datos sobre las acciones tomadas en respuesta a solicitudes de rectificación, actualización o eliminación en un plazo máximo de cinco días hábiles. Con este mismo periodo de tiempo cuentan los usuarios para notificar a los destinatarios, en caso de que sus datos sean cedidos o transferidos. Durante el proceso de corrección, el responsable del banco de datos debe bloquear el archivo o proporcionar información sobre el estado de revisión.

Sobre este tema, Basterra (2010) explica que los derechos de acceso, rectificación, eliminación, confidencialidad y cancelación de datos facilitan el ejercicio de otro derecho conocido como autodeterminación informativa. Este concepto se refiere a la capacidad del individuo, como propietario de sus datos personales, para decidir cómo serán utilizados y quién puede acceder a ellos. Por lo tanto, el artículo establece los derechos del titular sobre su información privada, así como las obligaciones que deben cumplir quienes la administran.

En consecuencia, dado que las bibliotecas recogen y procesan datos personales, deben garantizar el derecho de los individuos que utilizan sus servicios, a la corrección, actualización, confidencialidad o eliminación de su información personal contenida en sus bases de datos. Esto se alinea con lo expresado por la Asociación de Bibliotecas de Estados Unidos -ALA- (2006), que sostiene que, “en todas las áreas de la bibliotecología, las mejores prácticas permiten que los usuarios tengan el control de la mayor cantidad de opciones posible en lo que respecta a su privacidad.” (ALA, 2006, p. 6)

1.3. Archivos, registros, bases o bancos de datos. Usuarios y responsables

1.3.1. Formación de archivos, registros, bases o bancos de datos

El artículo 3 de la Ley 25.326 establece que la formación de archivos, registros, bases o bancos de datos sólo será lícita cuando “se encuentren debidamente inscriptos, observando en su operación los principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia" (p. 2)

Más adelante en el texto de esta legislación, el artículo 21 determina la obligación de los responsables de los archivos de datos a inscribirlos en el Registro dispuesto por el organismo de control correspondiente[7] y especifica que en caso incumplimiento, se aplicarán las sanciones especificadas en el artículo 31[8] de la Ley.

La finalidad de esta obligación es garantizar la transparencia en el tratamiento de datos personales y la protección de los derechos de los titulares de dicha información. Asimismo, Basterra (2013) afirma que lo establecido en el artículo 21 contribuye a brindar eficacia a la ley, conjuntamente con las sanciones que el organismo de control aplica en caso de incumplimiento.

Respecto a lo expresado anteriormente, se destaca el caso particular de las unidades de información que pertenecen a universidades nacionales, tratado brevemente en el estudio realizado por Temperini (2013) para el Observatorio Iberoamericano de Protección de Datos. En dicha investigación, se acudió al Registro Nacional de Bases de Datos Personales -en adelante RNBD- y se demostró que sólo 7 de las 46 universidades nacionales existentes tienen debidamente inscriptas algunas de las bases de datos que poseen y entre ellas se presenta el caso particular de la Universidad Nacional de Córdoba, que registra 7 de sus bibliotecas académicas. Por lo cual, se acentúa la necesidad de adecuar el tratamiento de los datos personales en instituciones educativas de nivel superior, para cumplir con lo establecido por la Ley 25.326.

1.3.2. Deberes de los responsables

La Ley 25.326 de Protección de los Datos Personales establece, en su artículo 9 las responsabilidades de los usuarios de los datos, al determinar que deben "adoptar las medidas técnicas y organizativas que resulten necesarias para

[7]La Dirección Nacional de Protección de Datos Personales -DNPDP- es la autoridad de aplicación de la Ley N° 25.326.

[8] ARTÍCULO 31. — (Sanciones administrativas).

1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos.

2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso. (Ley 25.326 Hábeas Data. Protección de Datos Personales, 2000)

garantizar la seguridad y confidencialidad de los datos personales" (p.4). Además, mediante el artículo 10 se añade que tanto el responsable, como las personas que intervengan en cualquier fase del tratamiento de datos personales, están obligados a mantener secreto profesional respecto a ellos.

Estas obligaciones surgen, de acuerdo a Masciotra (2020), como resultado de la actividad informática relacionada con el procesamiento de datos personales. Esto se debe al riesgo potencial de un uso inapropiado de la información registrada, que puede atribuirse tanto al gran volumen de datos como a la velocidad con la que se tratan. Por lo tanto, el responsable de los datos debe tomar las medidas apropiadas para salvaguardar la información personal almacenada, permitiendo así que los titulares ejerzan su derecho al acceso. Dichas medidas implican rediseñar formularios, adaptar estándares de comunicación y registro, proporcionar la formación adecuada al personal involucrado, entre otras.

En el contexto de las bibliotecas, el artículo 9 de la legislación previamente mencionada destaca la necesidad de desarrollar estrategias de protección de datos personales, considerando las particularidades de los servicios que brindan estas instituciones. Los cuales implican el uso de bases de datos que contienen datos personales de los usuarios, así como también los recursos consultados, préstamos, comunicaciones de referencia, transacciones y consultas digitales, además de registros relacionados con la utilización de servicios, programas e instalaciones de la biblioteca (ALA, 2006).

Cabe agregar, en relación a lo especificado en el artículo 10, que aun cuando se recaban datos personales no sensibles, es responsabilidad de los profesionales a cargo del registro, mantener la confidencialidad de dicha información. Como menciona Masciotra (2020), aquellos que "intervienen en cualquier fase del tratamiento de estos datos se les impone el deber de confidencialidad y secreto profesional". Asimismo, en este apartado de la Ley se hace mención del secreto profesional, el cual está ligado a la confidencialidad y, tal como lo expresa la IFLA (2012), es el concepto sobre el que se basa la relación entre la biblioteca y el usuario, siendo los profesionales de la información quienes deben tomar las medidas adecuadas para garantizar que los datos de los usuarios no sean compartidos por fuera del ámbito de servicio. Estas normativas y nociones permiten inferir que la

protección de datos personales es una cuestión con la que debe comprometerse la ética profesional de los bibliotecarios, a fin de brindar servicios de información que garanticen el derecho a la intimidad de los usuarios.

1.3.3. Contrato de servicios informatizados de datos personales

El artículo 25 de la Ley 25.326, establece que, en caso de brindarse servicios de tratamiento de datos personales mediante acuerdos con terceros, estos datos no podrán ser utilizados para un propósito diferente al establecido en el contrato de servicios ni ser compartidos con otras personas, ni siquiera para su conservación. Una vez finalizado el contrato, los datos personales procesados serán eliminados, a menos que la persona que contrató los servicios otorgue una autorización para realizar trabajos futuros. En ese caso, los datos podrán ser almacenados por un máximo de dos años.

Sobre estas disposiciones, Valesani et al. (2003) infieren que el responsable de los datos debe obligar por contrato a los prestadores de servicios de procesamiento a actuar según sus instrucciones para el tratamiento de la información y a cumplir con los deberes de confidencialidad y seguridad establecidos por la Ley 25.326. Por lo tanto, estas disposiciones apuntan a proteger la privacidad de los titulares de los datos y garantizar un uso responsable de la información personal en todos los ámbitos de su procesamiento.

Lo establecido por este artículo es de vital importancia en el campo de la bibliotecología, dado que con frecuencia se establecen acuerdos con empresas proveedoras de software y contenido para gestionar los diversos servicios que ofrecen las unidades de información. Frente a esto, la Organización Internacional de Estándares de Información -NISO, por sus siglas en inglés- (2015), confirma que es responsabilidad conjunta de las bibliotecas y proveedores de software, garantizar un entorno digital que tenga en cuenta las obligaciones éticas y legales de las bibliotecas y su personal, con el objetivo de proteger la privacidad de los usuarios de la biblioteca en sus datos personales, búsquedas, descubrimientos y uso de recursos y servicios.

En suma, como puede observarse en el desarrollo de este primer capítulo, la Ley de Hábeas Data es amplia y protege de manera integral los datos personales

que están vinculados a registros, archivos, bases de datos. Es relevante destacar que, dicha ley es el marco normativo que debería regir todos aquellos espacios institucionales donde se proceda a la recolección, tratamiento y uso de estos datos, entre ellos las bibliotecas universitarias, tanto públicas como privadas.

Capítulo 2: Normativa sobre protección de datos personales en el ámbito internacional. Los casos de América del Norte y Europa. Impacto sobre las bibliotecas de Estados Unidos, México y España

2.1. Organismos supranacionales. Protección de Datos Personales en bibliotecas

Dada la escasa literatura nacional encontrada respecto al tratamiento de datos personales en bibliotecas universitarias, los siguientes apartados de este capítulo se centran en analizar lo expresado por organismos supranacionales en este ámbito y los casos específicos de tres países: Estados Unidos, España y México, explorando su desarrollo en normativas sobre PDP, aplicadas posteriormente en bibliotecas. Con este propósito, se examinan declaraciones internacionales, legislaciones nacionales, directrices establecidas por organizaciones que nuclean a profesionales bibliotecarios y las investigaciones académicas que abordan esta temática.

Para comenzar, es necesario reafirmar que la PDP es un derecho fundamental contemplado en el artículo 12 de la Declaración Universal de los Derechos Humanos, según el cual “nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia (...). Toda persona tiene derecho a la protección de la ley contra tales injerencias” (Organización de las Naciones Unidas [ONU], 1948). Esto se replicó en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos[9] (1966) y en el artículo 11 de la Convención Americana sobre Derechos Humanos -Pacto de San José de Costa Rica-[10] (1968). Cabe aclarar que estas normativas fueron redactadas previamente al auge de las computadoras e Internet, por lo cual, la Observación General 16 del Comité de Derechos Económicos, Sociales y Culturales de las Naciones Unidas (1988), actualiza y profundiza lo anteriormente expresado, determinando que:

> La recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como

[9]Organización de las Naciones Unidas. (1966). *Pacto Internacional de Derechos Civiles y Políticos*. https://www.argentina.gob.ar/sites/default/files/derechoshumanos_publicaciones_colecciondebolsillo_06_derechos_civiles_politicos.pdf

[10]Organización de los Estados Americanos. (1968). *Convención Americana sobre Derechos Humanos*. https://shorturl.at/er8XH

> por las particulares o entidades privadas, deben estar reglamentados por la ley (...) Para que la protección de la vida privada sea lo más eficaz posible, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos. Si esos archivos contienen datos personales incorrectos o se han compilado o elaborado en contravención de las disposiciones legales, toda persona debe tener derecho a pedir su rectificación o eliminación. (p. 2)

De esta manera, se incorporan los nuevos medios en los cuales se procesa la información de las personas y que pueden significar un riesgo para su privacidad. Así como también, se incluye el derecho de los individuos a conocer y controlar la información que de ellos se almacena. Tal como lo expresa López Torres (2014), este documento introduce nociones referidas al derecho a la autodeterminación informativa. Es decir, el derecho de una persona a determinar qué se puede hacer o no con su información personal, abordando esencialmente las interrogantes de quién tiene acceso, de qué manera se accede y con qué propósito se utiliza dicha información.

Estos antecedentes, sentaron las bases para que la Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas -IFLA-, considerada como “el principal organismo internacional que representa los intereses de los servicios bibliotecarios y de información y sus usuarios” (IFLA, 2002), pudiera emitir numerosas declaraciones en donde se desarrollan estrategias para proteger este derecho en el ámbito de las bibliotecas. El primer trabajo que se puede mencionar es su “Manifiesto de la IFLA sobre Internet”, en el cual se establece que “las bibliotecas y los servicios de información deberían respetar la privacidad de sus usuarios y reconocer que los recursos que usan deberían permanecer

confidenciales” (IFLA, 2002, p.4). Más adelante, y en conjunto con la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura -UNESCO-, se amplía este documento y se desarrollan una serie de directrices para respaldar a los bibliotecarios en la formulación de políticas y en la identificación de prioridades que se ajusten a los servicios de Internet según las demandas de sus comunidades.

En primera instancia, dentro de este trabajo, la IFLA y UNESCO (2006) advierten que la privacidad de los usuarios se ve amenazada de manera más sencilla en el entorno de Internet, y que las políticas tradicionales de confidencialidad de las bibliotecas se encuentran en conflicto con las leyes promulgadas en múltiples países respecto a la necesidad de protección contra el terrorismo. Además, señala que no solo los gobiernos pueden representar una amenaza para la privacidad individual; las empresas también están altamente interesadas en analizar y comprender los patrones de navegación de los usuarios. Esta preocupación manifestada por la IFLA, especialmente respecto de la vigilancia por parte de instituciones gubernamentales, se intensifica a partir de las legislaciones sancionadas luego de los ataques terroristas de 2001. Tal como lo expresa Quispe Gerónimo (2003), estas normativas generaron polémica en la comunidad bibliotecaria mundial, dado que implicaban peligros para la libertad de información.

Asimismo, la IFLA y la UNESCO, en su publicación de 2006, profundizan en el concepto de privacidad y es referido como el derecho de los usuarios de bibliotecas a llevar a cabo búsquedas sin que otras personas examinen o accedan a sus temas de interés personal. Además, se entiende a la confidencialidad como las acciones que les permiten a las personas conservar el control sobre la información compartida con terceros y evitar el acceso no autorizado. Se destaca la noción de que la garantía del acceso a la información no debería ser a costa de la privacidad del usuario. Asimismo, se establece que las bibliotecas deben informar a los usuarios sobre sus políticas de privacidad, proteger su derecho a la protección de su intimidad al acceder y compartir información y proporcionar un entorno neutral que respete la individualidad de las personas que requieren sus servicios.

Más adelante, en el año 2012, la IFLA publica su código de ética destinado a bibliotecarios y otros trabajadores de la información, en donde determina que la relación entre la biblioteca y sus usuarios se fundamenta en la confidencialidad.

Sobre este texto, Ferreira Dos Santos (2019) comenta que, aunque existe un acuerdo general de que el respeto a la privacidad del usuario es un valor que todos los profesionales del mundo deben acatar, las asociaciones de cada país tienen la libertad de redactar sus propios códigos, adaptados a la realidad y al entorno en el que operan. No obstante, se considera que las directrices emitidas por la IFLA, se constituyen como una guía para la elaboración de políticas bibliotecarias, basadas en consensos internacionales, respecto a los temas que atañen a los profesionales de la información.

Cabe destacar que, en la “Declaración de la IFLA sobre la Privacidad en el Entorno Bibliotecario” (2015), se establece una conexión entre el artículo 19 de la Declaración Universal de Derechos Humanos, según el cual “todo individuo tiene derecho a la libertad de opinión y de expresión” (ONU, 1948), y el artículo 12 de la misma declaración, que establece la privacidad como un derecho humano fundamental. Esta asociación se basa en la premisa de que garantizar la privacidad es esencial para proteger el acceso a la información y la expresión de opiniones sin temor a posibles consecuencias negativas. Frente a la preocupación por afianzar estos derechos, se advierte que los proveedores comerciales de contenidos y servicios utilizados por las bibliotecas, ya sean de aplicaciones móviles, sistemas basados en la nube o softwares conectados a Internet, pueden recopilar información sobre las actividades, comunicaciones y transacciones de los usuarios. Por lo cual, desde las bibliotecas se debe negociar con proveedores para proteger la privacidad de la comunidad, rechazar servicios que recopilen demasiados datos o limitar el uso de tecnologías que comprometan el derecho a la intimidad. Frente a estas nociones, se añade que los servicios ofrecidos por las bibliotecas en colaboración con plataformas digitales, se encuentran en constante cambio y actualización, por lo cual es necesario revisar las políticas de privacidad de manera constante, para garantizar el resguardo de la privacidad de los usuarios.

Asimismo, en este documento, la IFLA (2015) emite una serie de recomendaciones, entre las que se destacan: la necesidad de que las bibliotecas colaboren con los esfuerzos nacionales, regionales e internacionales para proteger la privacidad y los derechos digitales; en caso de que se ofrezcan servicios que puedan comprometer la privacidad de los usuarios, darles la posibilidad de proveer un consentimiento informado; incluir a la protección de los datos en los programas

de alfabetización mediática e informacional destinada a usuarios; y contemplar la enseñanza de estrategias para garantizar la privacidad y confidencialidad en el ámbito bibliotecario como parte de la formación de los profesionales en bibliotecología. Estas recomendaciones evidencian el papel activo que deben asumir las bibliotecas y sus profesionales en temas actuales, tales como la protección de datos y regulación de servicios de Internet. Así lo afirma Ferreira Dos Santos (2019), al determinar que las unidades de información deben comprender, cuestionar y tomar medidas respecto a las tendencias emergentes, con el fin de construir un futuro colectivo basado en valores y metas compartidas.

Las declaraciones publicadas por la IFLA a lo largo de más de 21 años reflejan su profunda preocupación por incorporar la PDP como un deber fundamental de las bibliotecas. Esto se ha traducido en la elaboración de guías estratégicas, la creación de un código de ética y en un constante análisis de las oportunidades y amenazas que se presentan en este ámbito. Todo ello tiene como objetivo garantizar el derecho a la privacidad y la libertad de expresión.

Cabe agregar que este no es el único organismo internacional que se ha expresado sobre la temática. También se destaca la Asociación de Estados Iberoamericanos para el Desarrollo de las Bibliotecas Nacionales de los Países de Iberoamérica -ABINIA- (2023), según la cual, la privacidad de datos se define como el derecho que tienen las personas a mantener en reserva su información personal y tener la capacidad de controlar cómo se lleva a cabo la recopilación, el uso y el intercambio de esta información. Además, señala el ámbito de aplicación de esta garantía en las bibliotecas, que incluye registros de préstamos, búsquedas y la información personal proporcionada por los usuarios para acceder a servicios en línea. Más aún, asevera que la garantía de la privacidad de datos en las bibliotecas es un aspecto fundamental para preservar la confianza y la seguridad de los usuarios, ya que les permite realizar consultas sensibles y acceder a fuentes de información libremente y sin preocupaciones. De esta manera, acuerda con IFLA al establecer que la privacidad es un pilar fundamental para preservar la libertad intelectual y el derecho a la información.

Por lo tanto, los documentos analizados anteriormente evidencian que la protección de datos personales, un derecho fundamental respaldado por organismos

internacionales, se encuentra en el centro de la ética bibliotecaria. Tal es el caso de las entidades que representan a las bibliotecas y sus profesionales, como la IFLA y ABINIA, que están comprometidas con la confidencialidad y la preservación de la privacidad de los usuarios, impulsando la toma de medidas adecuadas para evitar la divulgación no autorizada de información personal.

2.2. La Protección de Datos Personales en Estados Unidos

En primer lugar, se opta por desarrollar el caso de Estados Unidos, ya que de acuerdo a la literatura analizada es “el país con el mayor número de pautas y la mayor profundidad con respecto a la privacidad de los usuarios de bibliotecas” (Ferreira Dos Santos, 2019, p. 47).

Sin embargo, es importante señalar que en este país no existe una ley específica a nivel nacional que regule la PDP, sino que, según Saldaña (2011), el Tribunal Supremo ha reconocido, a lo largo de un extenso período de jurisprudencia gradual, la mención implícita del derecho a la privacidad en la Constitución Federal de 1787 y sus Enmiendas. Esto incluye la protección de la libertad de asociación, establecida en la Primera Enmienda, que impide al gobierno obligar a revelar la afiliación a un grupo u organización. También se encuentra en la Cuarta Enmienda, que protege contra registros y confiscaciones sin causa justificada. Además, se extiende a la Quinta Enmienda, que resguarda contra la obligación de divulgar información personal, y a la Decimocuarta Enmienda, que garantiza el derecho de las personas a tomar decisiones fundamentales que afectan su vida personal y familiar sin interferencia estatal.

Por otra parte, en el ámbito educativo, prevalece la Ley de Derechos Educativos y Privacidad Familiar -FERPA, por sus siglas en inglés-, sancionada en 1974. Según el Buró Federal de Investigación -FBI- (s.f.), esta legislación federal tiene como objetivo salvaguardar la confidencialidad de los registros académicos de los estudiantes. La FERPA concede a los padres determinados derechos en relación a los registros educativos de sus hijos, y estos derechos se transfieren al alumno cuando alcanza la mayoría de edad, o cuando se matricula en una institución de educación superior. Las personas alcanzadas por esta normativa tienen derecho a examinar y modificar sus expedientes educativos, así como también, brindar autorización para la divulgación de la información contenida en los mismos. No

obstante, el alcance de la FERPA es limitado, ya que solo es aplicable en las entidades educativas que reciben financiamiento a través de cualquier programa del Departamento de Educación de los Estados Unidos (Quispe Gerónimo, 2002).

A pesar de que estas normativas ofrecen un marco de referencia para la PDP, la realidad es que la legislación estadounidense en esta materia se caracteriza por su fragmentación y corto alcance. Además, como señala Agüero Ovejero (2019), los trágicos ataques del 11 de septiembre de 2001 condujeron a la promulgación de la Ley Patriótica de EE. UU., que suspende y restringe ciertas libertades y derechos constitucionales con el propósito de fortalecer la seguridad interna y combatir el terrorismo. Particularmente en el caso de las bibliotecas, la cláusula 215 de esta legislación otorga al FBI la autoridad para solicitar a cualquier unidad de información en territorio nacional, la lista de libros que las personas requieren (Quispe Gerónimo, 2002).

En lo que respecta al ámbito bibliotecario, no se ha encontrado ninguna legislación federal que aborde de manera específica a la PDP en unidades de información. No obstante, resulta importante mencionar el caso del Proyecto de Ley de Protección de la Privacidad en Videos y Bibliotecas, presentado en 1988. El mismo, buscaba resguardar los registros de circulación, entrevistas de referencia, búsquedas en bases de datos, préstamos interbibliotecarios y otros registros identificables relacionados con el uso de servicios y materiales bibliográficos por parte de los usuarios de bibliotecas. De acuerdo a Bowers (2006), el FBI se opuso a este proyecto, dado que limitaba el alcance de sus investigaciones e influenció en la eliminación de todo lo referido a las bibliotecas en el contenido de esta normativa, que finalmente fue promulgada haciendo referencia únicamente a la prohibición de divulgación indebida de registros de venta o alquiler de materiales audiovisuales.

Asimismo, no puede dejarse de mencionar que el FBI puso en práctica, entre 1960 y 1970, el denominado Programa de Concientización Bibliotecaria, que consistía en un sistema de vigilancia enfocado en monitorear los hábitos de lectura de los usuarios y recopilar información sobre personas involucradas en actividades que eran consideradas como una amenaza para la seguridad nacional. Bowers (2006) sostiene que el FBI buscaba que los bibliotecarios proporcionarán

información sobre los patrones de lectura de personas extranjeras, especialmente de aquellos provenientes de la Unión Soviética.

Cabe destacar que el fuerte compromiso de los profesionales del área para con los principios de la PDP se evidencia en casos como “Los cuatro de Connecticut”[11], que se constituye como un ejemplo claro de los riesgos y amenazas a la privacidad de los usuarios de bibliotecas, el interés que puedan tener entidades gubernamentales sobre ellos y la actitud ética de los bibliotecarios respecto a la protección del derecho a la privacidad.

2.2.1. Asociación de Bibliotecas de Estados Unidos

Teniendo en cuenta el contexto descrito en el apartado anterior, es esencial resaltar a la Asociación de Bibliotecas de Estados Unidos -ALA- como una entidad que desempeña un papel central en la defensa del derecho a la PDP de los usuarios de unidades de información. Además, debido a que se trata de la “asociación bibliotecaria más antigua, más grande y más influyente en el mundo con 50.000 miembros” (ALA, 2017, párr. 1), su impacto a nivel internacional es considerable y se erige como un referente en este ámbito.

Esto se hace evidente, a través del artículo VII de la Declaración de los Derechos de las Bibliotecas, emitida por la ALA en 1939, según el cual:

> Todas las personas, independientemente de su origen, edad, antecedentes u opiniones, tienen derecho a la privacidad y confidencialidad en el uso de la biblioteca. Las bibliotecas deben defender, educar y proteger la privacidad de las personas, salvaguardando todos los datos de uso de la biblioteca, incluida la información de identificación personal. (párr. 8)

De acuerdo con Witt (2017), esta primera normativa aparece en paralelo al reconocimiento de la privacidad como un derecho legal en EE.UU., lo cual deja en evidencia el compromiso de la ALA por responder a las necesidades de brindar

[11]Christian, G., Bailey, B., Chase, P. y Nocek, J. (2008). Los cuatro de Connecticut. *Educación y biblioteca*, (166). 111-116. https://gredos.usal.es/bitstream/handle/10366/119540/EB20_N166_P111-117.pdf?sequence=1&isAllowed=y

garantías a los usuarios, en paralelo a las normas desarrolladas en aquel momento histórico.

En cuanto al contenido de esta declaración, se les ofrecen garantías a los usuarios, al explicitar los deberes de las bibliotecas respecto a la protección de datos personales. Además, según Zimmer (2014), se constituye a la privacidad como el elemento fundamental del derecho de una persona a acceder y recibir libremente ideas, información y puntos de vista, siendo un aspecto indispensable para fomentar y preservar la libertad intelectual. Por lo cual, se entiende que ninguna de estas libertades puede subsistir en un entorno donde la utilización de la biblioteca esté bajo vigilancia y las conductas de lectura y consulta se divulguen sin consentimiento. Solo cuando una persona tiene la certeza de que su elección de material de lectura está protegida, puede disfrutar plenamente de la libertad para explorar diversas ideas, evaluar argumentos y tomar decisiones.

El Código de Ética de la ALA (1939), en cuyo artículo 3 se vuelve a hacer referencia a esta temática, coloca como uno de los principios morales del ejercicio de la profesión bibliotecaria, al resguardo de la privacidad y confidencialidad de la información personal de los individuos que utilicen los servicios bibliográficos. Por lo cual, tal como lo expresa Zimmer (2014), proteger el ideal democrático de la libertad intelectual, traducido en el acceso libre y sin restricciones a la información es el principio esencial de la ética que promueve la ALA entre los bibliotecarios estadounidenses.

Más adelante, en 1971 se publica un documento que refiere a la "Política de confidencialidad de los registros bibliotecarios", en donde enfatiza la importancia de que todas las bibliotecas en los Estados Unidos desarrollen políticas que reconozcan el carácter confidencial de los registros de circulación y otros registros que revelen la identidad de los usuarios. Además, se destacó que estos registros no podían entregarse a agencias gubernamentales sin un proceso legal válido, como una orden judicial. En este caso, Witt (2017), señala que, durante los primeros años de la década de 1970, se produjo un aumento significativo en el interés sobre la privacidad dentro de comunidad bibliotecaria, como una reacción ante los esfuerzos de entidades del gobierno por emplear los historiales de préstamos de los usuarios,

con el fin de llevar a cabo investigaciones extensas para identificar posibles terroristas, debido a su interés en la fabricación de bombas.

Después de la publicación de este último documento, pasaron 31 años hasta que, en 2002, la ALA desarrolló un texto en donde se analiza y se acentúan ciertos conceptos expuestos en la Declaración de los Derechos de las Bibliotecas respecto a la protección de datos personales. Esto se puede atribuir a las consecuencias que tuvieron los ataques del 11 de septiembre de 2001 -como ya se expresara-, sobre legislaciones relativas a la privacidad, que encendieron las alarmas de los bibliotecarios estadounidenses y los pusieron en la necesidad de enfatizar sobre la responsabilidad de las bibliotecas en la protección de este derecho. A través del texto "Privacidad: una interpretación de la Declaración de Derechos de las Biblioteca", se remarca que todas las personas, sin importar su origen, edad, antecedentes o creencias, tienen el derecho a la privacidad y la confidencialidad en el uso de la biblioteca, cuando las garantías de libertad de investigación, expresión y pensamiento se ven comprometidas. Por lo cual, las unidades de información deben informar a los usuarios sobre sus políticas de recopilación de datos, controlar el registro de información no esencial y mantener políticas de privacidad actualizadas y seguras.

Continuando con esta perspectiva, en 2004, la ALA emite la “Política relativa a la confidencialidad de la información de identificación personal de los usuarios de la biblioteca”, en donde amplió la discusión al oponerse a cualquier uso del poder estatal para intimidar o reprimir individuos o grupos y promueve la resistencia contra tales abusos. Esto se debe a que declara haber observado visitas de agencias gubernamentales que buscan información personal de usuarios de la biblioteca, con el argumento de que lo que un individuo lee, puede reflejar su posicionamiento ideológico. Asimismo, en este documento se reconoce que las agencias pueden buscar registros de biblioteca en investigaciones criminales, pero remarca que esto solo debe hacerse a través de una orden judicial emitida por un tribunal competente después de demostrar una causa válida. Por lo tanto, se reafirma que las bibliotecas tienen la responsabilidad legal y ética de proteger la confidencialidad de todos los usuarios, incluidos los extranjeros.

Hacia el año 2006, con su “Resolución sobre la conservación de los registros de uso de la biblioteca”, la ALA instó a las unidades de información a tomar medidas específicas para proteger la privacidad del público, como limitar la recopilación y distribución de información de identificación personal y eliminar registros innecesarios. También promovió la realización de auditorías de privacidad anuales para garantizar el cumplimiento de las políticas. Más adelante, en 2007, emite un documento en donde reconoce la aplicabilidad de las Enmiendas Constitucionales mencionadas anteriormente en relación a las bibliotecas estadounidenses y destaca que 48 estados y el Distrito de Columbia tienen leyes que protegen la privacidad de los datos de las personas que utilizan las unidades de información. Sin embargo, dado que el contenido de estas legislaciones varía de un estado a otro y no existe una ley federal específica sobre PDP, la organización recomienda a cada biblioteca adoptar una política que respete las disposiciones de confidencialidad de su estado, reconozca la privacidad de la información solicitada o proporcionada por los usuarios, y garantice la privacidad de cualquier registro o información electrónica que revele los materiales consultados, prestados o adquiridos por los usuarios de la biblioteca. Por lo tanto, la diversidad de políticas de privacidad desarrolladas por las unidades de información estadounidenses es una respuesta a la fragmentación y la falta de uniformidad de las leyes, en lo que respecta a la protección de datos personales en este país.

Asimismo, se observa una reciente preocupación por los riesgos respecto a PDP que implican ciertas innovaciones tecnológicas aplicadas en bibliotecas. El primer caso ocurre en el año 2011, cuando se adoptó la “Resolución para Proteger la Confidencialidad de los Usuarios de Bibliotecas en las Prácticas de Autoservicio" en donde advirtió que se están introduciendo sistemas de autoservicio para la retención de materiales bibliográficos, los cuales no garantizan adecuadamente la protección de la privacidad de los usuarios. Frente a esto, se urge a las unidades de información a preservar el anonimato de los individuos mediante la implementación de prácticas que protejan la información de identificación personal asociada a los materiales prestados. Recientemente, en 2021, la ALA adoptó la "Resolución sobre el Uso Incorrecto de la Vigilancia de Datos de Comportamiento en Bibliotecas", en donde se aborda el problema de la recopilación de información sobre el uso que puede hacer una persona de los servicios de una unidad de información, con el

propósito de supervisar, rastrear o perfilar los hábitos de consumo de un individuo. Además, se reconoce que algunas bibliotecas enfrentan presión financiera para utilizar datos de usuarios, a fin de obtener beneficios por parte de proveedores de recursos. La resolución incluye una serie de medidas, como oponerse a la vigilancia de datos de comportamiento, instar a no intercambiar datos de usuarios por incentivos financieros y aplicar configuraciones de privacidad estrictas por defecto. También se hace un llamado a los trabajadores de bibliotecas para que defiendan los derechos de privacidad de los usuarios y se informen sobre ellos, de manera que actúen como custodios de la información personal, protegiéndola de un uso indebido y asegurando que no se explote ni se revele de manera no autorizada.

A partir de la lectura de los documentos anteriormente citados, puede observarse que la evolución de la preocupación de la ALA respecto a la protección de datos personales se ha mantenido en constante movimiento, de acuerdo a los desafíos que presenta el contexto histórico. De este modo, según Witt (2017), se evidencia que las medidas tomadas por esta asociación en cuanto a la PDP se vinculan al desarrollo de los criterios de privacidad en el ámbito profesional; la introducción de tecnologías innovadoras que cuestionan las concepciones sobre la confidencialidad; y las reacciones ante transgresiones de normas informativas vinculadas al contexto. Las emergencias más recientes se relacionan al uso de los datos personales como una mercancía en el mundo digital.

2.3. La Protección de Datos Personales en México

Con el propósito de analizar los enfoques adoptados por diferentes países latinoamericanos en el ámbito de las bibliotecas universitarias para garantizar la protección de los datos personales de los usuarios, de acuerdo con sus respectivas legislaciones, se opta por examinar el caso de los Estados Unidos Mexicanos. Debido a que, a través de su Constitución y dos leyes federales, se atiende a todo lo referido a esta temática desde una perspectiva que reconoce el derecho a la autodeterminación informativa. En esta sección, se explorarán lecciones destacadas derivadas de la experiencia mexicana.

En principio, Gómez Sánchez (2020) sostiene que la base del derecho a la protección de datos personales reside en el derecho a la privacidad, y como tal, ha estado presente en diversos documentos legislativos a lo largo de la historia del

derecho mexicano. Uno de sus antecedentes más antiguos se remonta a la Ley de Imprenta de 1917, que en su artículo 1° regulaba los ataques a la vida privada. Asimismo, este derecho se encontraba reflejado en el artículo 16 de la Constitución de 1917, donde se establece la protección a la privacidad al afirmar que nadie puede ser molestado en su persona, familia o domicilio. En julio de 2002, se promulgó la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), que determina los límites del derecho de acceso. En 2007, se incluyó por primera vez en la Constitución federal una referencia al derecho a la protección de datos personales, con el propósito de regular el ejercicio del acceso a la información. De este modo, el artículo 6° estableció los principios y fundamentos que guían la práctica de este derecho.

Recientemente, los avances dados por las Tecnologías de la Información y el Conocimiento, plantearon la necesidad de actualizar la Constitución Política para adaptarla a las nuevas necesidades de la población. Por lo cual, su artículo 6, modificado en 2014 y 2016, establece que la protección de la vida privada es un elemento indivisible del derecho a la información y, además, determina la potestad de las personas sobre sus datos. Más adelante, en su artículo 16 añadido en 2009 se declara que:

> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. (p. 17)

En cuanto a las legislaciones más recientes emitidas por México en materia de PDP, destacan la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), que rige sobre instituciones del sector privado, mientras que en el sector público existe la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), aprobada en el año 2018 y actualizada por última vez en 2021.

De acuerdo al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales -INAI- (s. f.), con la entrada en vigor de estas normativas, se establecieron una serie de principios comunes para ambos sectores -público y privado-, que determinan las reglas y obligaciones que rigen el tratamiento de datos personales por parte del responsable, a saber:

- **Licitud:** los responsables de los datos deben manejar la información de manera legal, conforme a la legislación y acuerdos internacionales, evitando cualquier tratamiento ilícito.

- **Consentimiento:** se requiere obtener el consentimiento para el tratamiento de datos, a menos que se apliquen excepciones establecidas por la normativa, es decir que los datos figuren en fuentes de acceso público; se sometan a un procedimiento previo de disociación, exista una situación de emergencia, entre otras. Para datos sensibles, se requiere un consentimiento expreso y por escrito.

- **Información:** los responsables deben informar a los titulares sobre el manejo que se hará de sus datos mediante un aviso de privacidad claro y comprensible.

- **Calidad:** los datos recolectados deben ser precisos, completos, pertinentes y actualizados según lo necesario para cumplir con la finalidad del tratamiento. Además, implica que la retención de datos no debe exceder el tiempo necesario para los fines originales.

- **Finalidad:** el tratamiento de datos debe limitarse a las finalidades establecidas en el aviso de privacidad. Estas deben ser específicas, claras y objetivas, evitando cualquier confusión sobre el propósito del tratamiento de datos.

- **Lealtad:** este principio impone la obligación de proteger los intereses del titular y su expectativa razonable de privacidad al tratar datos personales, se prohíbe la obtención de datos mediante medios engañosos o fraudulentos.

- **Proporcionalidad:** solo se deben tratar los datos necesarios para la finalidad justificada, limitando el tiempo de procesamiento de datos personales sensibles al mínimo necesario.

- **Responsabilidad:** los responsables deben asegurar el cumplimiento de estos principios, adoptando medidas y demostrando su aplicación ante titulares y autoridades.

Además de los principios y obligaciones mencionados, los responsables del sector público y privado están sujetos a los deberes de seguridad y confidencialidad. El deber de seguridad implica establecer medidas administrativas, físicas y técnicas para proteger los datos personales contra daño, pérdida, alteración o uso no autorizado. Las medidas administrativas incluyen capacitación del personal, las físicas se centran en la seguridad de espacios e infraestructura, y las técnicas protegen equipos contra virus. El deber de confidencialidad implica mantener en secreto los datos personales tratados, salvo con consentimiento o por obligación normativa. Para garantizarlo, se deben establecer medidas a lo largo de todas las fases del tratamiento, incluso después de finalizar la relación con el titular. El INAI es el organismo encargado de velar por el cumplimiento de estos derechos fundamentales.

En cuanto a las legislaciones específicas que abordan el ámbito de las unidades de información en México, es importante destacar que, aunque la Ley General de Bibliotecas no hace referencia a la protección de datos personales, en normativas regionales como la Ley de Bibliotecas de la Ciudad de México (2020) se establece que “las bibliotecas públicas reconocerán la libertad de investigar, y garantizarán su ejercicio con el respeto a la privacidad y la confidencialidad de lo que se investiga, protegiendo los datos personales en los términos establecidos en la ley respectiva” (Art. 5, p. 4). Esta legislación vincula directamente la salvaguarda de los datos personales con la garantía del derecho al acceso a la información, sin ningún tipo de restricción relacionada con la discriminación por sexo, etnia, edad o ideología. Por lo tanto, se comprende que la protección de datos personales se erige como una garantía fundamental para asegurar un acceso irrestricto al conocimiento.

Al considerar las normas anteriormente mencionadas, se puede inferir que las bibliotecas universitarias mexicanas, ya sean públicas o privadas, deben cumplir con

los deberes de seguridad y confidencialidad, e implementar estrategias para acatar los principios y obligaciones establecidos en la Constitución, la LFPDPPP o la LGPDPPSO, según corresponda, y las leyes regionales de acuerdo a su lugar de procedencia.

2.3.1. Colegio Nacional de Bibliotecarios de México

En el ámbito de las bibliotecas mexicanas, se destaca el Código de Ética Profesional del Colegio Nacional de Bibliotecarios de México, adoptado en 1991, que constituye un marco normativo que regula la conducta de los profesionales de la bibliotecología en el país. En 2014, el alcance nacional de este documento fue reconocido por la Asociación Mexicana de Bibliotecarios (AMBAC), el Consejo Nacional para Asuntos Bibliotecarios de las Instituciones de Educación Superior (CONPAB-IES) y la IFLA.

Por lo tanto, de acuerdo con Morán (2017), dicha normativa ética se reconoce como el documento más importante en materia de guía para el proceder profesional dentro de México, declarando el carácter obligatorio de lo estipulado, ya sea para aquellos que se gradúan de instituciones educativas nacionales o para aquellos que obtienen sus títulos en escuelas extranjeras en la misma disciplina.

El código se compone de nueve aspectos éticos, entre los que se destaca el “Respeto a la Confidencialidad”, según el cual, los bibliotecarios deben “guardar reserva de los hechos, respeto a la información solicitada o recibida, a los datos personales del usuario, así como a materiales consultados o prestados, a menos que lo autoricen los interesados” (Colegio Nacional de Bibliotecología, 2017, p. 2). Este principio se vincula directamente con las relaciones profesionales con los usuarios, según lo estipulado en el octavo aspecto ético del código. En el mismo se expresa que los bibliotecarios se comprometen a ofrecer “un trato amable, profesional objetivo y discrecional a todos los usuarios (...) y actuarán sin parcialidad ni discriminación considerando como confidencial toda información que se produzca durante la transacción profesional” (Colegio Nacional de Bibliotecología, 2017, pp. 2-3).

A pesar de este compromiso con la confidencialidad, es importante mencionar que el texto no hace referencia a las legislaciones sobre protección de datos

personales existentes en el país ni contempla el deber profesional de informar a los usuarios sobre sus derechos en relación con su Información privada, así como garantizar la formación continua del personal bibliotecario en estrategias de protección de datos. Además, no se encontraron otros documentos de igual alcance que reconozcan los derechos y responsabilidades en materia de protección de datos personales en el contexto de las bibliotecas mexicanas.

2.4. La Protección de Datos Personales en España

En este apartado se destaca la experiencia de España, considerando la exhaustividad y diversidad de legislaciones de alcance nacional e internacional que reglamentan la Protección de Datos Personales, tanto en este país, como en aquellos que forman parte de la Unión Europea.

En primer lugar, la Constitución española de 1978 reconoce en su artículo 18 que “se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen” y que “la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos” (p. 6). Por lo tanto, la legislación máxima de este país interpreta a la intimidad de los individuos como un derecho fundamental y establece la obligación de protegerlo principalmente de las intrusiones que se puedan realizar en el ámbito tecnológico.

Este artículo fue desarrollado en profundidad por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), la cual tenía como objetivo “garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar” (p. 4). Esta ley tuvo un alcance tanto en el sector público como en el privado, abarcando datos personales recopilados en formatos físicos y en cualquier otro medio.

Cabe destacar que, tal como lo señala García González (2007), esta normativa no hacía referencia al término “libertad informática” que recién apareció como derecho fundamental en la sentencia 292/2000 de 30 de noviembre pronunciada por el Tribunal Constitucional. En donde se lo define como el derecho a controlar el uso de estos datos dentro de programas informáticos e incluye la facultad de los individuos a oponerse al uso de ciertos datos personales para fines

diferentes a los que justificaron su recolección legítima. Por lo tanto, se entiende que la protección de la privacidad de las personas tiene una dimensión más amplia que el simple derecho a la intimidad establecido en el artículo 18.1 de la Constitución. Esta connotación positiva implica el derecho a controlar la información relacionada con uno mismo.

El 5 de diciembre de 2018, dicha normativa jurídica fue derogada en favor de la entrada en vigencia de la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales, la cual contempla las actualizaciones requeridas por la implementación del Reglamento General de Protección de Datos de la Unión Europea (RGPD). Esta regulación fue emitida con el propósito de unificar las políticas de protección de datos personales en Europa y se aplica a todas las organizaciones, tanto dentro como fuera de la región, que gestionen datos personales de ciudadanos residentes en la Unión Europea.

Entre sus artículos, la RGPD, estipula que, la administración pública debe respetar principios clave, tales como: “un tratamiento leal y lícito; limitación de la finalidad y una minimización de los datos y la retención.” (Directiva 95/46/CE. Reglamento general de protección de datos, 2016, p.115)

Por lo tanto, esta legislación busca garantizar el respeto de estos fundamentos y proveer la información necesaria para que las personas tengan conocimiento de su uso y tratamiento. Así como también, establecer medidas de protección ante el empleo indebido, difusión accidental, ilícita o sin consentimiento, de información personal, para que estos incidentes puedan ser subsanados en el corto plazo, informando al afectado de lo sucedido.

En lo que refiere a las bibliotecas, el RGPD protege a los usuarios que conforman la Unión Europea, a la vez que la Ley Orgánica de Protección de datos y Garantía de los Derechos Digitales (LOPDGDD) de 2018 establece un marco jurídico para la protección de datos en España.

Por otra parte, es importante destacar que éste país posee una legislación específica que atañe a las unidades de información: la Ley 10/2007, de 22 de junio, de la lectura, del libro y de las bibliotecas. En el artículo 12 inciso 2 de dicha normativa se sostiene que entre los valores de las bibliotecas se encuentra:

> El respeto del derecho de cada usuario a la privacidad y la confidencialidad de la información que busca o recibe, así como de los recursos que consulta, toma en préstamo, adquiere o transmite, protegiendo sus datos personales en los términos establecidos por las leyes. (p. 12)

Por lo tanto, España es el único país de los incluidos en esta investigación que ha promulgado una legislación en donde se especifique que la PDP es una garantía que deben ofrecer las bibliotecas.

Para finalizar éste apartado, se puede agregar que, según Varela-Orol y Ameneiros Rodríguez (2018) en las bibliotecas universitarias españolas, la referencia a sus políticas de privacidad puede hallarse en dos modalidades: minoritariamente a través de páginas web específicas sobre el tema o mediante enlaces a las páginas de las universidades en donde se enmarcan. A su vez, prevalecen dos denominaciones diferentes; esto es, lo que se reconoce como aviso legal o como política de privacidad. Cierto es que, hay un amplio espectro de bibliotecas que no ofrecen en su sede web ninguna información vinculada a políticas de privacidad. A lo sumo, en apartados como el de servicios, se menciona una declaración más bien genérica vinculadas al código de ética de la biblioteca.

En suma, parecería que persiste cierta disparidad en la protección de datos en el medio académico universitario español. Sin embargo, se reconocen y aplican los diferentes marcos normativos vigentes.

2.4.1. Federación Española de Sociedades de Archivística, Biblioteconomía, Documentación y Museística

La Federación Española de Sociedades de Archivística, Biblioteconomía, Documentación y Museística -en adelante, FESABID-, es una entidad privada fundada en 1988, que agrupa a 24 asociaciones y colegios profesionales, en España. Su objetivo es la promoción de intercambios de conocimientos y experiencias, contribuyendo para “lograr un crecimiento inteligente, sostenible e integrador de la sociedad” desde bibliotecas, archivos, museos y otras unidades de información. “FESABID es reconocida como portavoz común del colectivo profesional de la Información y la Documentación por las administraciones públicas,

la Unión Europea y diversos organismos internacionales". (Federación Española de Sociedades de Archivística, Biblioteconomía, Documentación y Museística, 2024)

Esta entidad posee un "Código de ética para bibliotecarios y profesionales de la información en España" desde 2013. En el mismo se establece que debe funcionar como una guía práctica para los profesionales, tanto del ámbito público y privado, que estén vinculados a la gestión de información y documentación. Es un documento que complementa el conocimiento especializado y la normativa técnica y legal, y orienta el ejercicio profesional responsable y de calidad.

Este código incluye expresamente legislación sobre reconocimiento de derechos humanos, especialmente los que están contenidos en la Declaración Universal de los Derechos Humanos, de acuerdo a su Preámbulo. Los artículos referidos a libertad, igualdad y dignidad de la persona; así como la libertad de expresión, opinión y acceso a la información. Para culminar con el derecho a la educación y la vida cultural, la protección de la propiedad intelectual y los derechos de autor.[12]

[12] **Artículo 1:** Todos los seres humanos nacen libres e iguales en dignidad y derechos y, dotados como están de razón y conciencia, deben comportarse fraternalmente los unos con los otros. **Artículo 2:** Toda persona tiene todos los derechos y libertades proclamados en esta Declaración, sin distinción alguna de raza, color, sexo, idioma, religión, opinión política o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición. Además, no se hará distinción alguna fundada en la condición política, jurídica o internacional del país o territorio de cuya jurisdicción dependa una persona, tanto si se trata de un país independiente, como de un territorio bajo administración fiduciaria, no autónomo o sometido a cualquier otra limitación de soberanía. **Artículo 3:** Todo individuo tiene derecho a la vida, a la libertad y a la seguridad de su persona. **Artículo 18:** Toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión; este derecho incluye la libertad de cambiar de religión o de creencia, así como la libertad de manifestar su religión o su creencia, individual y colectivamente, tanto en público como en privado, por la enseñanza, la práctica, el culto y la observancia. **Artículo 19:** Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión. **Artículo 26:** 1. Toda persona tiene derecho a la educación. La educación debe ser gratuita, al menos en lo concerniente a la instrucción elemental y fundamental. La instrucción elemental será obligatoria. La instrucción técnica y profesional habrá de ser generalizada; el acceso a los estudios superiores será igual para todos, en función de los méritos respectivos. 2. La educación tendrá por objeto el pleno desarrollo de la personalidad humana y el fortalecimiento del respeto a los derechos humanos y a las libertades fundamentales; favorecerá la comprensión, la tolerancia y la amistad entre todas las naciones y todos los grupos étnicos o religiosos, y promoverá el desarrollo de las actividades de las Naciones Unidas para el mantenimiento de la paz. 3. Los padres tendrán derecho preferente a escoger el tipo de educación que habrá de darse a sus hijos. **Artículo 27:** 1. Toda persona tiene derecho a tomar parte libremente en la vida cultural de la comunidad, a gozar de las artes y a participar en el progreso científico y en los beneficios que de él resulten. 2. Toda persona tiene derecho a la protección de los intereses morales y materiales que le correspondan por razón de las producciones científicas, literarias o artísticas de que sea autora. (Declaración Universal de los Derechos Humanos. 1948.) https://www.un.org/es/about-us/universal-declaration-of-human-rights

Entre sus preceptos se establecen:

- La privacidad y la confidencialidad para proteger los datos personales de “los usuarios de servicios de información y documentación con las únicas limitaciones que vengan determinadas por el marco jurídico.” (Federación Española de Sociedades de Archivística, Biblioteconomía, Documentación y Museística, 2024, p. 3)

- Poner a resguardo “la integridad y la autenticidad de la información y de la documentación suministrada.” (Federación Española de Sociedades de Archivística, Biblioteconomía, Documentación y Museística, 2024 p. 4)

- En pos de una gestión eficaz, mantenerse actualizados en lo que a “normas técnicas y legislación que afecta a las bibliotecas, archivos y centros de documentación.” (Federación Española de Sociedades de Archivística, Biblioteconomía, Documentación y Museística, 2024, p. 6)

- El respeto por “la información confidencial y la dedicación a actividades que sean competencia de la organización”. (Federación Española de Sociedades de Archivística, Biblioteconomía, Documentación y Museística, 2024 p. 6)

Por lo expresado hasta aquí, el código de FESABID reconoce la importancia de la protección de la privacidad al considerar que “la Información es un bien esencial en la sociedad”. (Federación Española de Sociedades de Archivística, Biblioteconomía, Documentación y Museística, 2024, p. 1)

Para finalizar, se observa que en España se tiende hacia la homogeneización en la protección de este tipo de datos, aunque persisten algunos desafíos. En contraste, en Estados Unidos y México, las normativas vigentes adoptan enfoques específicos según las necesidades y contextos particulares, reconociendo y protegiendo los derechos de los usuarios en función de demandas más específicas.

Capítulo 3: Las políticas y estrategias implementadas en las bibliotecas universitarias públicas y privadas relevadas de América y Europa

3.1. Políticas y estrategias de protección de datos personales de usuarios de bibliotecas. Contextualización y criterios de selección de las bibliotecas públicas y privadas de América y Europa

La PDP del usuario de bibliotecas, ha alcanzado cierto consenso como un valor que debe respetarse. Ahora bien, la promulgación de leyes de protección de datos en todo el mundo, así como la profundidad con la que se desarrolla el tema, varía de acuerdo al contexto de cada país y unidad de información, tal como se expuso en el capítulo anterior. Por lo cual, las bibliotecas de estos territorios, son libres de escribir sus propias políticas e implementar estrategias de PDP, adaptadas a la realidad y al contexto en el que están insertas.

Si bien, se asume que la protección del usuario debe estar garantizada, podría decirse que “no existe una receta para ser adoptada por todas las bibliotecas del mundo… El nivel de madurez de los instrumentos de protección legal varía en cada país.” Al mismo tiempo, “el perfil y los objetivos a largo plazo de las bibliotecas también pueden influir en la construcción de una política de protección de datos del usuario”. (Morán Guzmán y López Ruelas, 2019, p. 50)

De allí la relevancia de desarrollar en este capítulo, las medidas protectoras adoptadas por bibliotecas que se encuentran en los países presentados en el capítulo 2. El criterio implementado desde esta tesina para la selección de las unidades de información correspondientes a Estados Unidos, México y España, tanto públicas como privadas, se define teniendo en cuenta que, las universidades en las que se enmarcan están entre las 15 instituciones con mayor matrícula de cada país y/o que cuentan con políticas de privacidad destacadas.[13]

[13] En las siguientes páginas pueden observarse los datos de matrícula. En Estados Unidos, Universidad de California (2020): https://nces.ed.gov/programs/digest/d21/tables/dt21_312.10.asp. En México, Universidad Nacional Autónoma de México (2022): https://www.economia.gob.mx/datamexico/es/profile/institution/universidad-nacional-autonoma-de-mexico. En España Universidad Alfonso X el Sabio (2022): https://www.uax.com/noticias/la-universidad-alfonso-x-el-sabio-da-la-bienvenida-a-los-cerca-de-8.000-estudiantes-que-se-suman-este-curso-a-la-comunidad-uax

Así, en Estados Unidos: Biblioteca de la Universidad de California (pública), Biblioteca del Instituto Tecnológico de Massachusetts (privada). En México, Biblioteca de la Universidad Nacional Autónoma de México (pública) y Biblioteca de la Universidad La Salle (privada). Por último, en España Biblioteca de la Universidad de Cantabria (pública) y Biblioteca de la Universidad Alfonso X el Sabio (privada).

En el recorrido necesario para describir las políticas y estrategias de PDP que se implementan en las bibliotecas universitarias públicas y privadas seleccionadas de estos países, puede adelantarse como dato significativo que, en la mayoría de los casos, presentan tratamientos actualizados, contenidos en declaraciones, protocolos o informes elaborados por las unidades de información de acuerdo a las necesidades del servicio ofrecido.

3.2. Estados Unidos

3.2.1. Biblioteca Digital de la Universidad de California (pública)

La Biblioteca Digital de la Universidad de California (pública) establece explícitamente sus políticas y directrices en relación con la protección de datos personales, especialmente en el área de tecnología de la información. Este trabajo depende del departamento de Planificación, Programas y Coordinación Académica de la Oficina del Presidente de la universidad. Además, cuando corresponde, "desarrolla políticas específicas para su función dentro de la UC y las comunidades de bibliotecas digitales más amplias". (Biblioteca Digital de California, 2024, párr. 2)

En el marco de la Declaración de privacidad[14] con la que cuenta y, en particular, las prácticas en línea de la Biblioteca Digital de California -CDL, sigla en inglés-, actualizada a abril de 2024, se declara el reconocimiento al valor de la privacidad del usuario, explicando cómo se recopila, utiliza, divulga y procesa la información personal. Al hacer explícito que los datos que se recopilan son información personal del usuario, inician el recorrido por el tratamiento de los datos personales, los tipos de datos, limitaciones en la recolección y el uso de los mismos.

[14] La normativa legal que contiene a la presente Declaración de privacidad, enunciada en el mismo texto, hace referencia a: Ley de Prácticas de Información de 1977 (Sección 1798 del Código Civil y siguientes), la Ley de Registros Públicos (Sección 6250 del Código de Gobierno de California y siguientes) y la Sección 11015.5 del Código de Gobierno de California. California Digital Library. (2024). Declaración de privacidad. University of California. https://cdlib.org/about/policies-and-guidelines/privacy-statement/#personal-information-we-colle

Así, se expresa que: “Solo recopilamos información personal suya que sea relevante y necesaria para que podamos brindar servicios al público o que sea necesaria para cumplir con nuestras obligaciones según la ley”. (Biblioteca Digital de California, 2024, párr. 3)

Inmediatamente, la Declaración de privacidad, informa sobre qué tipo de información personal es la que recopila. Ésta incluye, la información que proporciona el usuario y la que se recopila automáticamente.

En cuanto a la primera, los datos mencionados son: nombre y apellido, dirección postal, dirección de correo electrónico, número de teléfono; comunicaciones en redes sociales con la biblioteca; código postal; afiliación profesional o académica y, otra información que el usuario esté dispuesto a brindar y que se utilizará de acuerdo con esta Declaración.

Respecto a la segunda, dirección de protocolo de Internet (IP), sistema operativo, tipo y versión de dispositivo, tipo y versión de navegador, identificación del navegador, páginas visitadas, frecuencia de acceso, tiempo dedicado a cada página, dirección de Internet del sitio que lo dirigió a nuestro Sitio y detalles del sitio web de referencia. Al mismo tiempo, información sobre su ubicación general, que puede determinarse a través de la dirección IP; sobre el dispositivo que utiliza para acceder al sitio web, como configuraciones únicas del dispositivo, sistema operativo, navegador, entre otros. (Biblioteca Digital de California, 2024)

Otra manera de recibir información personal, de acuerdo a esta Declaración, proviene de la recopilada por terceros. Los acuerdos con terceros pueden incluir a “nuestros socios comerciales, nuestros afiliados, nuestros socios comunitarios, nuestros proveedores de servicios, fuentes disponibles públicamente, incluidas las redes sociales en las que usted participa.” (Biblioteca Digital de California, 2024, párr. 5)

Cabe aclarar que, una vez definidos los enlaces y sitios o servicios de terceros, el texto menciona que “esta Declaración de privacidad no se aplica ni somos responsables de ninguna práctica de información personal de sitios web y servicios en línea de terceros o de las prácticas de otros terceros”. (Biblioteca Digital de California, 2024, párr. 6) Sin embargo, la biblioteca, al igual que la universidad,

protege la privacidad del usuario cada vez que sea posible ante el uso de contratos con proveedores, aunque se aclara que, las prácticas propias de estos sitios no tienen un control directo ni de la biblioteca como tampoco de la universidad. Por lo que se insta al usuario a visitar los respectivos avisos de privacidad de los servicios de terceros.

La protección de los datos y las estrategias implementadas, quedan explicitadas de la siguiente manera: la biblioteca “toma medidas de seguridad físicas, administrativas y técnicas apropiadas y razonables para preservar la integridad y seguridad de su información personal contra pérdidas, acceso no autorizado y uso o divulgación ilegal”. (Biblioteca Digital de California, 2024, párr.7) El almacenamiento de la información personal, se realiza en ubicaciones seguras. A la vez, quienes se desempeñan dentro de la biblioteca y tienen acceso a estos datos, “reciben capacitación sobre los procedimientos para la gestión de información personal, incluidas las limitaciones a la divulgación de información. El acceso a la información personal está limitado a aquellos miembros del personal de CDL cuyo trabajo requiere del mismo”. (Biblioteca Digital de California, 2024, párr. 7)

Los derechos de los usuarios, están mencionados en extenso:

- Acceder a su información personal;
- Rectificar o corregir información personal inexacta o incompleta que le concierne;
- Transferir su información personal a otro controlador o procesador;
- Hacer que se borre su información personal en determinadas circunstancias;
- Restringir el procesamiento de su información personal en determinadas circunstancias;
- Oponerse al procesamiento de información personal en determinadas circunstancias;

- Retirar su consentimiento para el procesamiento de su información personal, en caso de que UC solicite su consentimiento para el procesamiento de su información personal. (Biblioteca Digital de California, 2024, párr.14)

Posteriormente, la Declaración agrega que el usuario deberá confirmar su identidad al ejercer estos derechos, debido a la naturaleza confidencial del procesamiento de datos. Del mismo modo, “puede oponerse a las actividades de marketing por cualquier motivo y presentar una queja ante la autoridad local de protección de datos” (Biblioteca Digital de California, 2024, párr. 15), poniéndose en contacto con la biblioteca o la universidad.

En cuanto al consentimiento informado, se hace la salvedad que, habiendo obtenido dicho aval por parte del usuario, la biblioteca puede hacer uso del mismo y publicar dentro de los servicios que ofrece, sin vulnerar los derechos antes mencionados.

Así como el usuario tiene derechos, puede ejercer diferentes controles vinculados a sus datos personales. En este caso, está delimitado a: preferencias de comunicaciones por correo electrónico y la modificación o eliminación de la información. Respecto al uso del correo electrónico, el acceso que tiene la biblioteca permite el envío de avisos relacionados con el sitio y el servicio. Pero el usuario puede cancelar la suscripción y dejar de recibir notificaciones.

No obstante, se establece que: “no puede optar por no recibir comunicaciones relacionadas con el servicio (por ejemplo, verificación de cuenta, comunicaciones transaccionales, cambios/actualizaciones de características de los Servicios, avisos técnicos y de seguridad).” En el mismo sentido, se notifica al usuario que puede optar por eliminar la información personal y, se hace la aclaración de que: “es posible que no podamos modificar o eliminar su información en todas las circunstancias”. (Biblioteca Digital de California, 2024, párr. 16)

A la vez, explicita las advertencias sobre riesgos cuando hace referencia a: la retención de información personal, el contrato que la universidad y la biblioteca tienen con los datos del público y su tratamiento y la actualización de las prácticas

de privacidad. Tal y como sostiene el documento, se conserva la información personal de las personas tiempo necesario o permitido por la ley, con la finalidad para la cual se obtuvo. Esto puede variar si cambia el acuerdo/contrato entre el usuario y la biblioteca o en función de los requerimientos legales.

Como la universidad oficia de controlador de los datos personales de los que dispone, en relación con el uso de acuerdo a los servicios brindados, puede utilizarlos cuando sea necesario siempre que “no haya un impacto primordial en sus intereses o derechos. En algunos casos, podemos pedirle que nos otorgue su consentimiento por separado para utilizar su información personal”. (Biblioteca Digital de California, 2024, párr. 17)

Por último, cada vez que la Declaración de privacidad se actualiza, se espera del usuario la revisión periódica de la página para mantenerse informado. La vigencia de las prácticas de privacidad coincide con la fecha de la última actualización, la que se identifica al inicio de la página. Y aclara que “su uso continuado de los sitios después de cualquier cambio en esta Declaración constituirá su aceptación de dicho cambio”. (Biblioteca Digital de California, 2024, párr. 17)

Para cerrar este apartado, puede advertirse que las políticas y estrategias de PDP implementadas por la Biblioteca Digital de California, reúnen las características necesarias para un ejercicio seguro del acceso del usuario y sus datos personales a este servicio.

3.2.2. Biblioteca del Instituto Tecnológico de Massachusetts (privada)

La Biblioteca del Instituto Tecnológico de Massachusetts -privada, siglas en inglés MIT-, presenta su política de seguridad de datos de los usuarios con una última actualización en noviembre de 2020. En lo que a tratamiento de los datos personales se refiere, la biblioteca asume el compromiso de proteger la privacidad y confidencialidad de los individuos cuando visitan o utilizan sus servicios. La política de PDP implementada detalla cómo se manejan los datos personales del público y el marco legal que la contiene, ya mencionados en el capítulo 2[15]. Al mismo tiempo, se

[15] Su privacidad en el MIT también está cubierta por la Política de Privacidad del MIT, que complementa esta política, y la Política del MIT 11.0 Privacidad y Divulgación de Información Personal . La protección legal de su privacidad proviene de una variedad de leyes (algunas de las cuales, según su ciudadanía, lugar de residencia y el tipo de información involucrada, pueden aplicarse a sus interacciones con las Bibliotecas), que incluyen: FERPA, HIPAA, las regulaciones y la ley de violación

describe en un apéndice destinado a tal fin, la definición de lo que la biblioteca entiende como “información de identificación personal” -PII, en inglés-.

> Hemos adoptado la definición de “Datos personales” del Reglamento General de Protección de Datos (GDPR) como base de la Información de Identificación Personal (PII) que recopilamos en las Bibliotecas. Esa definición es “cualquier información relativa a una persona física identificada o identificable; Una persona física identificable es aquella que puede identificarse, directa o indirectamente, en particular mediante un identificador como un nombre, un número de identificación, datos de ubicación, un identificador en línea o uno o más factores específicos del estado físico, fisiológico, identidad genética, mental, económica, cultural o social de esa persona natural”. (*MIT Libraries*, 2020, párr. 26)

Esta modalidad de información al público permite que sepa sobre aquello que se recopila, de qué manera se usa, cómo protege y cuándo puede compartirse aquel conjunto de datos recabados, aclarando que son solo aquellos necesarios para que la biblioteca pueda brindar eficientemente sus servicios. Al mismo tiempo, hace referencia explícita a otorgarle opciones para controlar aquellos datos brindados. Ofrece herramientas que ayudan a salvaguardar los datos, como por ejemplo, que la biblioteca cuente con computadoras para los usuarios externos, brindando así una opción de acceso, en cierto modo, más anónimo (*MIT Libraries*, 2020). Tal como se explica en el documento:

> Si es particularmente sensible a la privacidad, el uso de computadoras de acceso público puede proporcionar una capa adicional de anonimato a su uso. La actividad de navegación en dispositivos personales a veces puede

---

de datos, el Reglamento General y las regulaciones de violación de datos de otros estados de EE. UU. Las prácticas de privacidad de las Bibliotecas del MIT y esta política también se han basado en muchos estándares y guías bibliotecarias, incluidas las de la Asociación Estadounidense de Bibliotecas , la Federación Internacional de Asociaciones de Bibliotecas y la Organización Nacional de Estándares de Información. (MIT Libraries, 2020, s.d.)

> estar vinculada a usted, incluso cuando no ha proporcionado voluntariamente su información personal. El uso de una computadora pública reduce ese riesgo y puede considerar la posibilidad de anonimizarse aún más mediante el uso de herramientas. (*MIT Libraries*, 2020, párr. 17)

En lo que respecta a la recopilación de datos y su tratamiento, ya se adelantó cuáles son los solicitados y bajo qué marco legal. Aquí cabe agregar que los datos recopilados, “se clasifican utilizando pautas publicadas por el Programa de Seguridad de la Información Escrita, que determinan cuánto tiempo se conservan y cómo se almacenan. Esta clasificación coloca a los sistemas en categorías de riesgo bajo, medio o alto”. (*MIT Libraries*, 2020, párr.19) Mientras que los datos de bajo riesgo, pueden ya ser públicos o bien, su divulgación no sería perjudicial para el usuario; los datos de alto riesgo pueden estar vinculados a requisitos de tipo legales, causando -su circulación-, perjuicios tanto en cuestiones de seguridad, de índole financiera u operativos. De más está decir que, los datos de riesgo medio, apelan a algunos de estos aspectos, entre medio de la calificación.

La compilación de los datos, de acuerdo a esta biblioteca, puede realizarse desde diferentes fuentes, a saber: aquellos que son proporcionados directamente por el público, entregando su ID o interactuando -en forma personal o virtual- con el personal de la biblioteca; datos brindados a través de las herramientas vinculadas a los diferentes servicios de la biblioteca; información que deviene sobre usuarios de otros sistemas o por proveedores externos, considerados aquí como datos que se proporcionan de forma agregada.

Ahora bien, ¿quiénes tienen acceso a los datos recopilados, dentro del personal de la biblioteca? Una vez establecidos los rangos de riesgo de la información recabada, los datos más sensibles solo son accesibles al personal que necesita interactuar con ellos para realizar algún tipo de acción. Por ejemplo, la biblioteca cuenta con un servicio de anonimización para los datos de alto riesgo de los usuarios individuales, convirtiéndolos así en un riesgo menor. Mientras tanto, "los datos de riesgo medio pueden ser accesibles a todo el personal de las Bibliotecas, o pueden limitarse a individuos o grupos específicos, según corresponda". (*MIT Libraries*, 2020, párr. 19) En el caso de los datos de bajo riesgo, la biblioteca puede

divulgarlos públicamente de manera razonable, esto es, anulando la identificación antes de publicarlos, a menos que el usuario permita lo contrario.

Avanzando en el análisis de la Política de privacidad de datos de los usuarios de la Biblioteca del Instituto Tecnológico de Massachusetts, los acuerdos con terceros están contemplados para los casos en que se utilicen proveedores para brindar servicios bibliotecarios. En tal caso, la información procesada por terceros debe regirse por la política de seguridad vigente, ya que se les exige el mismo nivel de privacidad y seguridad sobre los datos personales de los usuarios que en la biblioteca. Además, la unidad de información auténtica cada interacción con una plataforma de terceros, permitiendo así su acceso.

En otro orden, ya tratado en el capítulo 2, en referencia a las intromisiones gubernamentales en las bibliotecas en décadas pasadas, aquí se establece que “la información sobre los usuarios individuales de la biblioteca no se pondrá a disposición de ninguna agencia del gobierno estatal, federal o local”. (*MIT Libraries*, 2020, párr. 21) La excepción a ésta normativa, está dada solo por órdenes judiciales de debido proceso y que serán notificadas al usuario por un funcionario autorizado de la organización solicitante.

Al llegar a este punto, es necesario ampliar sobre la utilización, modificación o eliminación de registros de datos. En primer lugar, la biblioteca establece que la información brindada se utiliza para proporcionar y mejorar los servicios solicitados. Además, se aclara que la biblioteca no vende la información recopilada a ninguna otra organización (*MIT Libraries*, 2020). Por otra parte, la conservación de estos datos depende de la clasificación de riesgo previamente mencionada, así como de la necesidad operativa de dichos datos. El uso activo de la información para los objetivos por los que fue otorgada expira luego de un período específico y se procede a su eliminación.

En cuanto a la salvaguarda de los datos y la advertencia sobre riesgos, si bien ya se ha tratado a lo largo de este apartado, cabe agregar aquí, lo que sigue. La integridad y seguridad de los datos que la biblioteca protege, se realizan a través de diferentes vías que se refuerzan mutuamente para garantizar la PDP. De acuerdo al documento en análisis:

> En primer lugar, intentamos recopilar el conjunto mínimo de información necesaria para proporcionar el servicio solicitado. En segundo lugar, seguimos las recomendaciones de seguridad pertinentes para garantizar la seguridad de los datos que recopilamos. En tercer lugar, descartamos su información personal tan pronto como sea posible y factible. (*MIT Libraries*, 2020, párr. 28)

Al mismo tiempo, se suman como recomendaciones de seguridad “los estándares de cifrado relevantes y actualizaciones rápidas para abordar las vulnerabilidades del sistema. El alcance de estas prácticas está informado por la clasificación de riesgo aplicable a cada tipo de datos” (*MIT Libraries*, 2020, párr. 28). En este contexto, la selección de los proveedores de servicios de terceros que puedan contribuir a la infraestructura digital es muy cuidadosa.

Lo expresado hasta aquí, deja en claro que tanto la salvaguarda de los datos como la advertencia sobre riesgos, es un objetivo primordial de esta biblioteca, cuando se consideran todas las estrategias aplicadas para la PDP.

Para finalizar este apartado, cabe mencionar el reconocimiento de los derechos de los usuarios, plasmado como un incentivo desde la Introducción de la Política de privacidad desarrollada por las bibliotecas del MIT: ¡Le animamos a conocer y ejercer sus derechos de privacidad! (*MIT Libraries*, 2020, párr. 1) Posteriormente, se enumeran, las garantías que poseen las personas que utilizan sus servicios:

1. Acceso: tiene derecho a obtener una copia de los datos sobre usted que almacenamos.

2. Rectificación: tiene derecho a corregir la información inexacta o completar la información incompleta.

3. Eliminación: tiene derecho a que se eliminen sus datos personales previa solicitud (a menos que se apliquen determinadas circunstancias).

4. Restricción u objeción al procesamiento: puede solicitar que limitemos el procesamiento de su información personal o que dejemos de procesar su información personal (bajo ciertas condiciones).

5. Portabilidad de los datos: puede solicitar que transfiramos los datos recabados a otra persona o directamente a usted. (*MIT Libraries*, 2020, párr. 11)

En cuanto a la responsabilidad sobre la política de privacidad, la biblioteca sostiene un inventario de sistemas donde realiza un seguimiento de la información almacenada sobre los usuarios. Su frecuente revisión aborda amenazas sobre la privacidad, las que son subsanadas por el personal de la biblioteca. Estos últimos, reciben capacitaciones sobre privacidad, en tanto y en cuanto, son quienes están en contacto frecuente con los datos de las personas. Por esto, son responsables de mantener la vigencia de la política de privacidad aquí desarrollada.

Por último, los cambios en la normativa vigente se informan con un aviso destacado en los sitios web de la biblioteca y se aplican a partir de la fecha de aprobación. Sin embargo, si el usuario lo solicita, se pueden aplicar medidas de protección de privacidad de forma retroactiva.

3.3. México

3.3.1. Biblioteca Central de la Universidad Nacional Autónoma de México (pública)

La Dirección General de Bibliotecas y Servicios Digitales de Información -en adelante DGBSDI- de la Universidad Nacional Autónoma de México -que actualiza sus funciones en 2022-, es responsable de recabar datos personales de los usuarios, del tratamiento de los mismos y de su protección, así como de su resguardo.

En cuanto al tratamiento de los datos, en el Aviso de Privacidad Integral de la Dirección General de Bibliotecas y Servicios Digitales de Información (DGBSDI) de la Universidad Nacional Autónoma de México, se declara que cualquiera sea el rol a

desempeñar dentro de la biblioteca, ya sea: estudiante, docente, personal, investigador, visitante, entre otros-, los datos recabados serán utilizados para todas o algunas de las siguientes finalidades; entre las que se destacan:

- Prestar servicios bibliotecarios y de información, así como de vigilancia;
- Actualizar, capacitar y practicar exámenes al personal que labora en las bibliotecas;
- Dar un seguimiento personalizado a las solicitudes de información de los siguientes servicios y trámites:
    a. Acceso remoto
    b. Análisis de citas
    c. Búsquedas especializadas
    d. Constancia de no adeudo para titulación UNAM
    e. Educación continua
    f. Obtención de documentos
    g. Servicio bibliotecario para personas con discapacidad en la Biblioteca Central
- Ofrecer la difusión de conocimientos científico, tecnológico y profesional.
- Actualizar la base de datos de alumnos, estudiantes, docentes y empleados, así como sus respectivos contactos en caso de emergencia.

- Identificar a los alumnos cuando soliciten un préstamo bibliotecario y cuenten con adeudos por retraso en la entrega de acervo documental. (Biblioteca Central UNAM, 2022, párr. 1)

La información personal es recabada utilizando los mecanismos remotos de las plataformas virtuales, las que mencionan como las oficiales.[16] A la vez, se especifica el tipo de datos personales que se obtienen, agrupados en tres categorías, a saber:

- Identificativos, como nombre y apellido, domicilio, fecha de nacimiento, nacionalidad, teléfono, correo electrónico, grado académico, entre otros.
- Laborales, donde puedes distinguirse: empleado, autoempleado, desempleado. En el caso del primero se solicita -además de los que identifican al usuario, la relación laboral vinculada a la profesión que ejerce; mientras que, para el segundo y tercer caso, se suman los motivos por los cuales no trabaja y el tiempo que lleva sin empleo.
- Y académicos, con un registro de niveles alcanzados, tiempo que tomó la titulación, dominio de otros idiomas, habilidades desarrolladas, entre los más relevantes, además de los que permiten la identificación del usuario. (Biblioteca Central UNAM, 2022)

En cuanto al uso de datos y la presencia de consentimiento expreso, ambos conceptos giran en torno a los datos personales sensibles. En este caso, el Aviso de Privacidad Integral, deja establecido que: “Cuando se recaben datos personales sensibles, se le solicitará su consentimiento expreso y por escrito para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca.” (Biblioteca Central UNAM, 2022, párr. 3) Se realiza la salvedad de los casos que están previstos en el marco de la Ley

[16] Plataformas virtuales implementadas por la UNAM para recabar datos, según consta en el Aviso de Privacidad Integral (Biblioteca Central UNAM, 2022, s.d.):

- https://www.dgb.unam.mx
- https://www.bibliotecas.unam.mx/
- https://www.bidi.unam.mx
- https://econtinua.dgb.unam.mx/
- https://www.bibliotecacentral.unam.mx/

General de Protección de Datos Personales en Posesión de Sujetos Obligados, la que fuera presentada en el capítulo 2 de esta investigación.

Si bien las finalidades para las que se hará uso de los datos personales ya se destacan al inicio del Aviso de Privacidad Integral, un poco más adelante el mismo documento retoma el "Fundamento para el tratamiento de datos personales". En este caso, para ratificar los marcos legales que contienen dicha temática, y como ya se explicitó en el apartado 2.3, se alude a la Constitución Política de los Estados Unidos Mexicanos. Al mismo tiempo, agregan los Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México, publicados en la Gaceta UNAM el 25 de febrero de 2019.[17]

El Aviso de Privacidad Integral que se viene analizando en este apartado, no describe aspecto alguno referido a acuerdos con terceros.

Sin embargo, como novedoso pueden agregarse aquí las webs *beacons*. Éstas refieren a técnicas que son utilizadas por la biblioteca para registrar "la actividad del usuario en cuanto al acceso a cierto tipo de información dentro del sitio Web con propósitos estadísticos y de mejora del sitio." (Biblioteca Central UNAM, 2022, párr. 5) Este registro de actividad del usuario, no se encuentra presente en otros documentos sobre privacidad de PDP relevados.

Y continúa delimitando cuáles son los tipos de información registrados con las webs *beacons*, a saber:

- Tipo de navegador y sistema operativo.
- Si cuenta o no con software como *java script o flash*.
- Sitio que visitó antes de entrar al nuestro.
- Vínculos web que sigue en Internet.
- Su dirección IP (*Internet Protocol*). (Biblioteca Central UNAM, 2022, párr. 5)

[17] Si bien los Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México, no hacen mención a la Biblioteca Central de la UNAM, la que se viene tratando en este apartado, es destacable lo minucioso del documento en cuanto a PDP. Puede consultarse en: https://www.red-tic.unam.mx/content/acuerdo-por-el-que-se-establecen-los-lineamientos-para-la-proteccion-de-datos-personales-en

La Biblioteca Central UNAM, entre sus declaraciones, pone especial énfasis en los derechos de los usuarios, el acceso, modificación o eliminación de registros y sobre la advertencia sobre riesgos. Tal es así que los denominan y desarrollan como el “Ejercicio de derechos ARCOP (Acceso, Rectificación, Cancelación, Oposición y Portabilidad al uso de sus datos personales).” (Biblioteca Central UNAM, 2022, párr. 8)

En lo que a acceso se refiere, el usuario tiene derecho a saber qué tipo de datos personales tiene la biblioteca, para qué son utilizados y en qué condiciones se realiza. En cuanto a la rectificación, se específica que “es su derecho solicitar la corrección de su información personal en caso de que esté desactualizada, sea inexacta o incompleta.” (Biblioteca Central UNAM, 2022, párr. 8)

Ante el uso inadecuado de los registros o bases de datos, el usuario puede solicitar la cancelación de los mismos; así como ejercer el derecho a oposición, en cuanto al uso de sus datos para fines específicos y, “solicitar la transmisión de sus datos personales en un formato estructurado y comúnmente utilizado a otro responsable, cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato (Portabilidad).” (Biblioteca Central UNAM, 2022, párr. 8)

Para el ejercicio pleno de estos derechos se consigna a dónde acudir, a través de una página sugerida; así como se informa al usuario el tiempo en que será comunicada la determinación adoptada por la biblioteca, si resultara procedente.

Un aporte más en cuanto al consentimiento informado, similar a los ya expresados en otros documentos, es que el usuario puede revocar el permiso otorgado para el tratamiento de sus datos personales, teniendo en cuenta que no en todos los casos se podrá atender a la solicitud o suspender el uso de forma inmediata. Su revocación “implicará que no le podamos seguir prestando el servicio del sistema en línea que nos solicitó, o la conclusión de su relación con nosotros.” (Biblioteca Central UNAM, 2022, párr. 11)

Finalmente, cabe destacar que las modificaciones al Aviso de Privacidad se publican en el sitio oficial de la unidad de información. Por ello, se recomienda consultar dicho sitio al menos semestralmente para estar al tanto de las condiciones y términos

actualizados. De nuevo, el papel del usuario en su propia información y formación es fundamental.

3.3.2. Biblioteca de la Universidad La Salle (privada)

Al llegar a este punto cabe aclarar que, luego de relevar las 97 universidades privadas de la ciudad de México y, a la vez, verificar que sus bibliotecas cuenten con documentación específica sobre la PDP que permita describir los aspectos sobre los que se construye este capítulo, es decir: tratamiento de los datos personales; tipos de datos y limitaciones en la recolección y uso de datos; salvaguarda de los datos; acuerdos con terceros; derechos de los usuarios; consentimiento informado y formación; acceso, modificación o eliminación de registros y advertencia sobre riesgos. Se observa que casi la totalidad de ellas delegan el resguardo y protección de la privacidad sobre datos personales a la declaración de la universidad a la que pertenecen. Sin hacer, aclaraciones pertinentes, dentro de estos documentos, sobre el servicio que le es propio a la biblioteca.

En el único caso donde se encuentra una referencia específica es en la Universidad La Salle -privada-, que en sus Políticas de Privacidad[18] recorta la actividad propia de su biblioteca universitaria, expresando:

> El servicio de préstamo de material (libros, periódicos, audiolibros, videos, etc.) de la Coordinación de Biblioteca utilizará los datos personales de los alumnos para mantener un registro histórico de préstamos, adeudos de material y multas relacionadas, que se describen con mayor detalle en los Lineamientos del Centro de Multimedios, el titular autoriza al hacer uso de los servicios de este centro a dar seguimiento a las multas hasta su pago total. (Universidad La Salle, 2020, párr. 6)

Como puede observarse, solo se hace mención a la utilización de datos personales en lo que a préstamo de materiales corresponde.

[18] *Nota de la autora:* Al ingresar en la página de la biblioteca universitaria https://biblioteca.lasalle.mx/, se identifica al final de la misma, el Aviso de Privacidad, desde allí se remite a las Políticas de Privacidad de la Universidad La Salle de donde se extrae el párrafo presentado.

3.4. España

3.4.1. Biblioteca de la Universidad de Cantabria (pública)

La Biblioteca de la Universidad de Cantabria -pública- cuenta con un documento específico para la actividad de la unidad de información en lo que a PDP se refiere. Actualizado en 2023, la Información sobre protección de datos personales (RGPD arts. 13 y 14) -RGPD ya tratado en el capítulo 2, apartado 2.4.-, describe como novedoso -desde estos dos artículos-, que quien es responsable del tratamiento de los datos debe informar al usuario qué tipo de datos y cuál será su uso tanto en el caso de que los datos personales se obtengan del interesado -art. 13-, como cuando no hayan sido conseguidos directamente del usuario -art. 14-. (Biblioteca de la Universidad de Cantabria, 2023)

Dentro de la Información básica sobre protección de datos (2023), los tipos de datos se presentan a continuación del interrogante: "¿Cómo hemos obtenido sus datos?", y se especifica:

> Los datos personales objeto de tratamiento son los que usted nos ha facilitado. En caso de que usted pertenezca o haya pertenecido a la Universidad de Cantabria, sus datos pueden proceder de otros ficheros de la propia UC.
>
> Las categorías de datos que tratamos son:
>
> a) Datos de carácter identificativo: NIF/DNI, Nombre y apellidos, Dirección, Teléfono, Firma/Huella, dirección de correo electrónico.
>
> b) Otros tipos de datos: - Características personales: Fecha de nacimiento. - Académicos y profesionales: Profesión, pertenencia a colegios profesionales o asociaciones, centro de matriculación y estudios, puesto de trabajo y departamento –para miembros de la comunidad universitaria–. (Biblioteca de la Universidad de Cantabria, 2023, párr. 16)

Aquí corresponde recordar lo ya explicitado para el caso de que los datos no sean obtenidos directamente del usuario, situación en la que se observan las mismas prescripciones.

Con el mismo formato, se responde a "¿Con qué finalidad tratamos sus datos personales?" para establecer las limitaciones en la recolección, uso de datos y su tratamiento: "Tratamos los datos personales que nos facilita –o de los que disponemos en caso de pertenecer ya a nuestra comunidad universitaria– para la gestión de los servicios de la biblioteca, en particular el préstamo y acceso a bases de datos." (Biblioteca de la Universidad de Cantabria, 2023, párr. 11) También se especifica que no serán utilizados para la elaboración de perfiles, no serán comunicados a ningún otro personal que no sea el propio de la comunidad, ni otra finalidad que exceda las actividades habituales de la biblioteca, como por ejemplo: gestión de préstamos, acceder a las instalaciones y usar recursos disponibles, así como "encuestas de calidad de los servicios del sistema de calidad institucional, entre otras." (Biblioteca de la Universidad de Cantabria, 2023, párr. 1)

En otro párrafo, se amplía lo ya expresado acerca de qué manera se legitima el tratamiento de los datos brindados y queda explicitado que se forma a los usuarios sobre esta temática. Siendo la biblioteca la responsable del tratamiento de los datos de los miembros de la comunidad universitaria, "de ello se informa convenientemente en el ingreso en la indicada comunidad universitaria". (Biblioteca de la Universidad de Cantabria, 2023, párr. 12)

Al mismo tiempo, y como otro aporte novedoso desde esta biblioteca en cuanto a consentimiento informado y formación, se elabora un Informe adicional sobre protección de datos en el mismo protocolo, donde se agrega que cuando el usuario accede a la comunidad universitaria, en el momento de recoger los datos, el responsable del tratamiento de los mismos, pone a disposición información adicional donde:

> Se informa de las condiciones completas del tratamiento, conforme al Reglamento Europeo de Protección de Datos, por lo que su pertenencia a la comunidad universitaria o su solicitud de alta como usuario de la Biblioteca supone una clara acción afirmativa de consentimiento, cumpliendo por tanto

las exigencias de consentimiento del citado reglamento. (Biblioteca de la Universidad de Cantabria, 2023, párr. 12)

En cuanto al acceso, modificación o eliminación de registros, no se pone tiempo límite para la conservación de los datos recabados, -sin embargo, más adelante se hace mención al bloqueo de los mismos por determinadas situaciones-. En efecto, bajo salvaguarda de la reglamentación como marco legal, los datos se conservan en la biblioteca salvo que el usuario solicite su eliminación. (Biblioteca de la Universidad de Cantabria, 2023)

El acuerdo con terceros, hace referencia a que, se han establecido contratos o actos jurídicos que comprometen a “las empresas encargadas del mantenimiento de las aplicaciones informáticas que gestionan los servicios de la Biblioteca” (Biblioteca de la Universidad de Cantabria, 2023, párr. 13) en los que se establecen las condiciones y las garantías necesarias para el resguardo y protección de los datos personales.

En el marco de los derechos de los usuarios y advertencia sobre riesgos, se aporta en general el acceso, la rectificación y supresión de los datos. Luego, en el Informe adicional sobre protección de datos, se amplía:

1) Usted tiene derecho a:

- Solicitar el acceso a los datos personales que tratamos sobre usted.
- Solicitar su rectificación o supresión.
- Solicitar la limitación de su tratamiento.
- Oponerse a su tratamiento.
- Portabilidad de sus datos. (Biblioteca de la Universidad de Cantabria, 2023, párr. 14)

Avanza el informe sobre el derecho a retirar el consentimiento prestado para el tratamiento de datos personales, haciendo la siguiente aclaración:

No obstante, deberá tener en cuenta lo siguiente:

a) La retirada del consentimiento respecto al Servicio de Biblioteca de la UC, supone que usted no podrá seguir utilizando estos servicios.

b) Asimismo, la Universidad de Cantabria procederá al bloqueo de los datos cuando considere que pueden ser necesarios para procedimientos administrativos o judiciales posteriores durante el tiempo en que puedan producirse los mismos. (Biblioteca de la Universidad de Cantabria, 2023, párr. 14)

En suma, la Biblioteca de la Universidad de Cantabria presenta aportes significativos para la PDP, como las analizadas hasta aquí, sumando novedosas contribuciones en cuanto a información y formación de usuarios.

3.4.2. Biblioteca de la Universidad Alfonso X el Sabio (privada)

En junio de 2021, la Biblioteca de la Universidad Alfonso X el Sabio -privada-, actualiza su Política de Privacidad como responsable del tratamiento de datos personales, destinada a toda la comunidad universitaria. El marco legal que lo contiene, -el que fuera presentado en el capítulo 2 para España-, se encuentra respaldado por el Reglamento General (UE) de Protección de Datos (RGPD), la Ley de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD). (Biblioteca de la UAX, 2021)

En el segundo párrafo del documento bajo análisis, con un formato personalizado, la biblioteca confirma que con esta Política de Privacidad: “queremos explicarle, de forma sencilla, clara y transparente, cómo tratamos y protegemos su información personal y sus derechos. Su seguridad y la de sus datos personales es fundamental para nosotros y nos tomamos muy en serio su adecuada protección”. (Biblioteca de la UAX, 2021, párr. 2)

Queda establecida la relevancia que, para esta biblioteca, y la universidad a la que pertenece, tienen la protección y salvaguarda de los datos personales, así como también la seguridad del usuario. Inmediatamente en el párrafo 3, cuando se hace referencia a la posibilidad de modificar esta política se especifican los motivos: “para

adaptarla a novedades legislativas, doctrinales o jurisprudenciales (…) o por motivos técnicos, operativos, comerciales, corporativos y de negocio" (Biblioteca de la UAX, 2021, párr. 3)

A lo expresado se agrega que la publicación de las modificaciones se realizará debidamente y recomienda que: "cada vez que se acceda a esta Plataforma, se lea con detalle esta política". (Biblioteca de la UAX, 2021, párr. 4) Como en el caso analizado anteriormente, se focaliza en la responsabilidad del usuario de mantenerse informado.

En lo referido al tratamiento de los datos personales contenida por la normativa vigente y aplicable en materia de PDP -ya presentada-, aquí se menciona específicamente que:

> Los datos personales obtenidos durante la navegación por el sitio web biblioteca.uax.es, y especialmente mediante la cumplimentación y envío de los formularios que se ponen a su disposición en este sitio, corporativo y en otros vinculados a subdominios uax.es y con enlace a la presente política de privacidad, serán tratados por la entidad Universidad Privada de Madrid, S.L. (UAX) (Biblioteca de la UAX, 2021, párr. 5)

En cuanto a tipos de datos, limitaciones en la recolección y uso, se establece que serán recabados por los diferentes formularios web dispuestos para tal fin y según la finalidad para la que están siendo solicitados. No obstante, se aclara que: "siempre le solicitaremos aquellos datos personales que resulten adecuados, pertinentes y limitados a lo necesario". (Biblioteca de la UAX, 2021, párr. 7)

Para dicha recolección, la biblioteca establece un conjunto de categorías, a saber:

- Datos personales identificativos directos.
- Datos personales de contacto.
- Datos sobre características o circunstancias personales.

- Datos académicos.
- Datos profesionales.
- Datos económicos y/o bancarios.
- Datos relativos a la salud vinculados a la gestión de citas médicas en el ámbito de la Clínica UAX. (Biblioteca de la UAX, 2021, párr. 7)

Específicamente, en cuanto al uso que se realiza de los datos personales, éste se relaciona con el cumplimiento de las obligaciones legales y contractuales que están vinculadas a las diferentes actividades que se realizan en la UAX, tales como docencia, investigación, divulgación académica e institucional y los servicios administrativos. En cualquier caso, el uso será remitido en los avisos informativos de la biblioteca. En este punto, la Política de Privacidad enumera un extenso listado sobre el uso específico de datos, haciendo expresa mención a la "base de legitimación" de cada uso, entre los que se destacan:

- Registro y gestión de su cuenta personal como miembro de la Comunidad UAX. Base de legitimación: consentimiento expreso del interesado.
- Gestión académica. Base de legitimación: ejecución de contrato de prestación de servicios educativos en el que el interesado es parte.
- Gestión contable, económica, fiscal y administrativa derivada de las transacciones vinculadas a los servicios prestados. Base de legitimación: ejecución de contrato de prestación de servicios en el que el interesado es parte, así como cumplimiento de obligaciones legales derivadas de la aplicación de la legislación en materia fiscal, contable y administrativa.

- Comunicaciones necesarias con alumnos. Base de legitimación: Existencia de interés legítimo derivado de la relación establecida con UAX y ejecución de contrato de prestación de servicios en el que el interesado es parte.

- Gestión de becas privadas y tramitación de becas públicas. Base de legitimación: Cumplimiento de obligaciones legales. (Biblioteca de la UAX, 2021, párr. 8)

Tal y como puede observarse, no sólo se hace referencia al uso de datos en forma general, sino que también se destaca la inclusión en cada uno de ellos de la "base de legitimación", como información relevante para el usuario.

Aquí se describen los acuerdos con terceros, aclarándose que, los datos personales pueden ser accesibles tanto a proveedores como prestadores de servicios externos. En este caso, quienes ocupan el lugar de encargados del tratamiento de los datos, son los terceros que, según se manifiesta, están obligados por contrato a seguir los lineamientos expuestos en materia de PDP. El control de dichas acciones -que incluye inspecciones y auditorías- está a cargo de las autoridades de la UAX, "para comprobar que tales encargados del tratamiento cumplen de forma estricta con sus obligaciones legales y contractuales en materia de protección de datos personales". (Biblioteca de la UAX, 2021, párr. 10)

Los derechos de los usuarios están reconocidos en la normativa vigente, ya referida al comienzo de este apartado. De acuerdo a esto la Política de Privacidad los destaca de la siguiente manera:

- Derecho a solicitar el acceso a los datos personales relativos al interesado.

- Derecho a solicitar la rectificación de los datos incorrectos.

- Derecho a solicitar la supresión de sus datos.

- Derecho a solicitar la limitación del tratamiento.
- Derecho a oponerse al tratamiento.
- Derecho a la portabilidad de sus datos.
- Derecho a no ser objeto de decisiones individuales automatizadas.
- Revocación del consentimiento. (Biblioteca de la UAX, 2021, párr. 13)

A diferencia de los análisis realizados con anterioridad en las bibliotecas seleccionadas para el desarrollo de este capítulo, puede destacarse aquí la mención a la limitación u oposición por parte del usuario al tratamiento de sus datos personales. Así como de evitar ser objeto de decisiones automatizadas e individuales.

En cuanto a la conservación y/o eliminación de registros, la Política de Privacidad advierte que, “cuando los datos personales ya no resulten necesarios para los fines de tratamiento para los que fueron recabados se procederá a su supresión de modo que no puedan ser tratados -ni siquiera visualizados-”. (Biblioteca de la UAX, 2021, párr. 11) Cabe destacar aquí, la inclusión de la no visualización en ninguna plataforma o red vinculada a la UAX.

El caso de excepción para la no supresión o conservación de los datos personales recabados, se vincula a disposiciones de tipo legales -jueces y tribunales, particularmente de las autoridades de protección de datos-. En esta situación, los datos se conservarán debidamente bloqueados para ser tratados por las autoridades competentes y con un plazo preestablecido por la normativa vigente. (Biblioteca de la UAX, 2021)

Por último, la advertencia sobre riesgos aplica a las medidas de seguridad y protección de los datos personales que toma en cuenta la institución. Y queda debidamente explicitado:

Teniendo en cuenta la naturaleza, el ámbito, el contexto y los indicados fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para

> sus derechos y libertades, UAX aplica (y aplicará) medidas, técnicas y organizativa, apropiadas a fin de garantizar la debida seguridad y protección de sus datos personales, atendiendo a criterios de privacidad desde el diseño y por defecto, así como aplicando un sistema de enfoque al riesgo concurrente que se revisará y actualizará por UAX cuando sea necesario. (Biblioteca de la UAX, 2021, párr. 12)

Los actos de protección esbozados se apoyan en las probabilidades y amenazas que pueden representar riesgos diversos, tanto a los derechos del usuario como a sus libertades. En tal sentido, la labor que se realiza en torno a la debida seguridad y protección de los datos personales atiende a cada uno de los criterios incluidos en la Política de Privacidad, aplicando un sistema integral ante el riesgo que pueda presentarse en la simultaneidad de los mismos.

Por último, cabe destacar la inclusión de la relevancia del rol del personal de la institución en cuanto a la PDP. En efecto, el documento menciona no sólo al personal administrativo; sino que suma al académico, quienes cuentan con "formación e información en materia de protección de datos, y específicamente cómo tratar la información que contenga datos personales, qué realizar en su puesto de trabajo y cómo actuar ante cualquier incidente en esta materia". (Biblioteca de la UAX, 2021, párr. 12) En este caso, el desempeño del personal que está al frente del servicio de la Biblioteca de la Universidad Alfonso X el Sabio, adquiere una relevancia particular. Lo que estaría indicando la necesidad de la capacitación continua en PDP para alcanzar la eficiencia y eficacia en su resguardo dentro de las unidades de información.

Capítulo 4: Presentación y análisis de los datos

4.1. Metodología implementada

El tipo de estudio que se emplea a los fines de desarrollar la presente tesina es exploratorio-descriptivo dado que, de acuerdo a lo expresado en el estado del arte de esta investigación, no se hallaron trabajos académicos que aborden las estrategias que aplican las bibliotecas universitarias argentinas para garantizar el cumplimiento de la Ley 25.326 de Protección de los Datos Personales. Asimismo, no se recuperaron documentos referidos a políticas de privacidad disponibles en las sedes web de bibliotecas universitarias argentinas públicas y privadas, ni tampoco fue posible descubrir normas vigentes de asociaciones representantes de bibliotecas y bibliotecarios en donde se haga referencia a la ética profesional en el manejo de datos personales de usuarios.

Por esto, es exploratorio cuando, como en este caso, examina un tema sobre el que no hay abordajes académicos que puedan relevarse. Siguiendo las definiciones de Hernández Sampieri et al. (2014): “Los estudios exploratorios se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado (…) o que no se ha abordado antes” (p. 91).

Al mismo tiempo, es descriptivo, dado que busca especificar cómo se implementa el tratamiento y la protección de los datos personales en bibliotecas argentinas públicas y privadas.

La estrategia metodológica elegida es de tipo mixta, la cual puede definirse como:

> “la integración sistemática de los métodos cuantitativo y cualitativo en un solo estudio con el fin de obtener una “fotografía” más completa del fenómeno. Éstos pueden ser conjuntados de tal manera que las aproximaciones cuantitativa y cualitativa conserven sus estructuras y procedimientos originales” (Hernández Sampieri et al., 2010, p. 546).

Por lo tanto, este estudio emplea una estrategia cualitativa inicial, para profundizar en aspectos teóricos, con el objetivo de ampliar el conocimiento sobre la

temática y establecer las variables clave a investigar. A partir de estos conceptos se desarrolla la herramienta de recolección de datos, utilizando un enfoque cuantitativo. La información obtenida se analiza teniendo en cuenta las legislaciones, normativas y estrategias de PDP estudiadas con anterioridad. Finalmente, se formulan sugerencias para la aplicación de la Ley 25.326 de Hábeas Data en las unidades de información argentinas.

Mediante esta estrategia, como indica Creswell (2005), citado por Hernández Sampieri et al. (2010), se busca “obtener una mayor variedad de perspectivas del problema: frecuencia, amplitud y magnitud (cuantitativa), así como profundidad y complejidad (cualitativa); generalización (cuantitativa) y comprensión (cualitativa)”. (p. 550)

El objeto de investigación de la presente tesina son bibliotecas de universidades públicas y privadas de la República Argentina. Los criterios de selección que se aplican para determinar las unidades de análisis, obedecen a dos momentos: en primer lugar, se inicia por el territorio argentino con aquellas provincias que cuenten con sedes centrales de universidades públicas y privadas. Realizado este relevamiento, en segundo lugar, se hace foco sobre las instituciones con las matrículas más altas, para establecer una biblioteca universitaria pública y otra privada por cada jurisdicción.

En este punto cabe aclararse que 12 provincias de la República Argentina, a saber: Catamarca, Chaco, Chubut, Formosa, Jujuy, La Pampa, La Rioja, Neuquén, Río Negro, San Luis, Santa Cruz y Tierra del Fuego no poseen universidades privadas con sede central en sus territorios. Frente a esta realidad, se seleccionan como unidades de análisis las siguientes jurisdicciones que cumplen con los criterios establecidos anteriormente: Buenos Aires, Ciudad Autónoma de Buenos Aires -CABA-, Córdoba, Corrientes, Entre Ríos, Misiones, Mendoza, Salta, San Juan, Santa Fe, Santiago del Estero y Tucumán. De modo que, para este estudio se pueda consultar a igual número de unidades de información tanto de universidades públicas, como privadas, tal y como puede verse en las siguientes tablas:

	PROVINCIA	UNIVERSIDAD PÚBLICA	BIBLIOTECA
1	**BUENOS AIRES**	Universidad Nacional de La Plata	**BPUNdeLP**
2	**CABA**	Universidad Nacional de Buenos Aires	**BFdeCE**
3	**CÓRDOBA**	Universidad Nacional de Córdoba	**BFdeFH**
4	**CORRIENTES**	Universidad Nacional del Nordeste	**BC "PÍJLM"**
5	**ENTRE RÍOS**	Universidad Nacional de Entre Ríos	**BC "PAS"**
6	**MISIONES**	Universidad Nacional de Misiones	**BdeFdeHyCS**
7	**MENDOZA**	Universidad Nacional de Cuyo	**B "DOMC"**
8	**SALTA**	Universidad Nacional de Salta	**BCdeFCEJyS**
9	**SAN JUAN**	Universidad Nacional de San Juan	**BCdelaFdeCS**
10	**SANTA FE**	Universidad Nacional de Rosario	**BFdeCEyE**
11	**SANTIAGO DEL ESTERO**	Universidad Nacional de Santiago del Estero	**BCUNdeSdelE**
12	**TUCUMÁN**	Universidad Nacional de Tucumán	**B "PJA"**

Tabla 1: Provincias, universidades nacionales y bibliotecas argentinas. **Fuente:** Elaboración propia.

	PROVINCIA	UNIVERSIDAD PRIVADA	BIBLIOTECA
1	**BUENOS AIRES**	Universidad FASTA	**BUFASTA**
2	**CABA**	Universidad Argentina de la Empresa	**BUADE**
3	**CÓRDOBA**	Universidad Empresarial Siglo 21	**BC**
4	**CORRIENTES**	Universidad de la Cuenca del Plata	**BUdelaCdelP**
5	**ENTRE RÍOS**	Universidad Adventista del Plata	**B “EIM”**
6	**MISIONES**	Universidad “Gastón Dachary”	**BCM**
7	**MENDOZA**	Universidad de Mendoza	**BSC**
8	**SALTA**	Universidad Católica de Salta	**BCS**
9	**SAN JUAN**	Universidad Católica de Cuyo	**B “MDM”**
10	**SANTA FE**	Universidad del Gran Rosario	**SR**
11	**SANTIAGO DEL ESTERO**	Universidad Católica de Santiago del Estero	**BCODL**
12	**TUCUMÁN**	Universidad del Norte Santo Tomás de Aquino	**BSCT**

Tabla 2: Provincias, universidades privadas y bibliotecas argentinas. **Fuente:** Elaboración propia.

Para la recolección de datos se realiza una encuesta semiestructurada (Ver Anexo) dirigida al área de referencia de cada una de las unidades de información, con el propósito de explorar en profundidad y complejidad de qué manera estas instituciones gestionan la información personal de sus usuarios, en función de la legislación nacional vigente.

A fin de establecer las dimensiones y variables aplicables al instrumento de relevamiento de datos de esta investigación, se procede a seleccionar aquellos conceptos clave que se reiteran dentro del marco teórico planteado. Esto permite organizar con mayor claridad los resultados.

Por tanto, las dimensiones y variables en torno a las que se organiza la encuesta son:

DIMENSIONES	VARIABLES
NORMATIVA	- Marco legal - Políticas de privacidad
DATOS	- Tipos de datos - Utilidad de los datos - Conservación y eliminación de datos
USUARIOS	- Derechos de los usuarios - Consentimiento
SIGB Y SERVICIOS WEB	- Sistemas Integrados de Gestión Bibliotecaria - Correo electrónico - Redes sociales - Acuerdos con terceros
FORMACIÓN DE USUARIOS Y DEL PERSONAL BIBLIOTECARIO	- Capacitación de los usuarios sobre PDP - Capacitación personal bibliotecario sobre PDP

Tabla 3: Dimensiones y variables. **Fuente:** Elaboración propia.

4.2. Relevamiento y presentación de los datos

Construido y aplicado el instrumento de recolección de datos, se procede a la presentación de los resultados, agrupados por dimensiones, variables y su respectiva pregunta. En todos los casos las respuestas son abordadas por cantidad de bibliotecas. Se decide agrupar por las devoluciones de coincidencia mayoritaria, en cada variable de las respuestas recibidas y, considerar por separado, aquellas donde no hay similitudes, caso en el que se transcriben las observaciones realizadas por las bibliotecas.

Cabe aclarar que, de las 24 encuestas enviadas, 12 a bibliotecas de universidades privadas y 12 a bibliotecas de universidades públicas, se recibieron 16 respuestas, 8 por cada tipo de unidad de información.

4.3. Respuestas obtenidas

La pregunta 1, refiere a la identificación de la biblioteca como pública o privada.[19]

4.3.1. Dimensión Normativa

VARIABLE	PREGUNTA/S
MARCO LEGAL	**2. ¿Se menciona la aplicación de la Ley 25.326 de Protección de los Datos Personales en algún documento oficial de la biblioteca (Reglamento, Manual de Procedimientos, Estatuto, Protocolo, etc.)? Especificar.**

En el caso de las **bibliotecas universitarias públicas**, cinco unidades de información respondieron negativamente. Mientras que tres especificaron lo siguiente:

[19] Nota de la autora: la pregunta 1 se fórmula considerando que, si bien las encuestas se enviaron a las unidades de información previamente relevadas, algunos encuestados podrían responder desde sus correos electrónicos personales. Frente a estos casos, esta pregunta facilita la identificación del tipo de institución a la que pertenecen.

- **BC “PAS”:** se hace mención a la aplicación de la Ley 25.326 en el “Manual de Procedimiento, Estatuto y Protocolo”.
- **BC “PÍJLM”:** “se menciona en un apartado del reglamento de administración y gestión del repositorio institucional de la universidad”.
- **BFdeFH:** “se menciona en la RHCS-UNC 1365/2017 Políticas Institucionales de la UNC para el Repositorio Institucional RDU-UNC, en el apartado 6. políticas de resguardo de datos personales”.

Por otra parte, el 75% (seis) de las **bibliotecas universitarias privadas** respondieron negativamente y el 25% (dos) estableció que dicha legislación se menciona en el reglamento de la unidad de información.

VARIABLE	PREGUNTA/S
POLÍTICAS DE PRIVACIDAD	**3. ¿Disponen de políticas de privacidad especialmente diseñadas por y para la biblioteca?** ● Sí____ Continua a la pregunta 3.1 ● No___ Continua a la pregunta 4 **3.1. Estas políticas de privacidad, ¿se encuentran disponibles en la web para los usuarios?** ● Sí ● No **3.2. ¿Con qué frecuencia se actualizan las políticas de privacidad?** ● Nunca ● Rara vez ● A veces ● Casi siempre ● Siempre **3. 3. ¿Se notifica a los usuarios de dichas actualizaciones? *** ● Sí____ Continua a la pregunta 4 ● No____ Continua a la pregunta 4

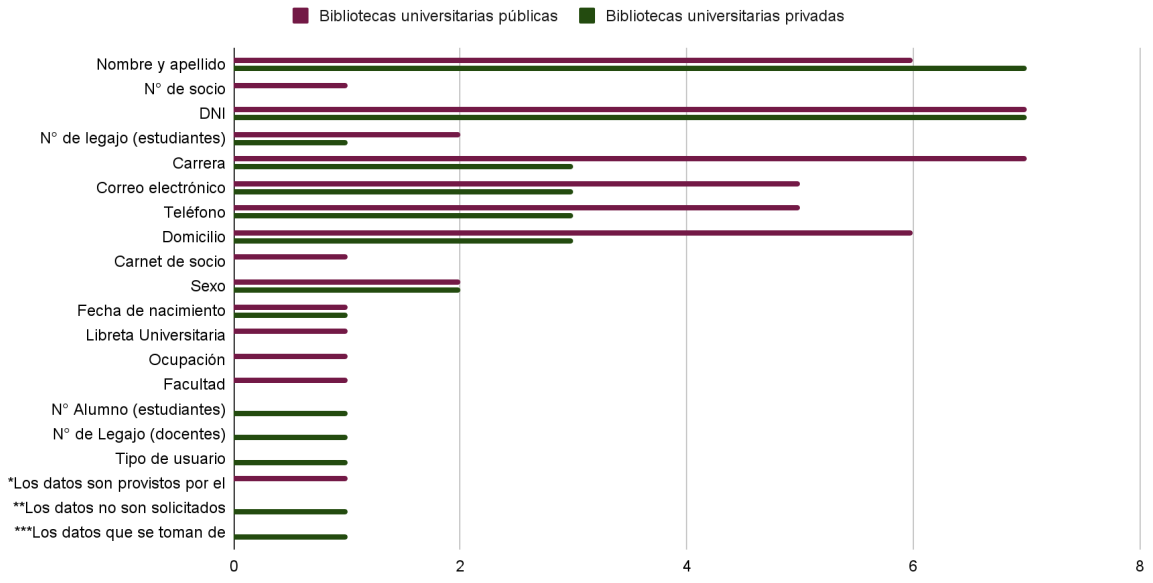
A la pregunta 3, ocho **bibliotecas universitarias públicas** respondieron negativamente. Frente a esto, las preguntas 3.1, 3.2 y 3.3 no obtuvieron respuestas.

Por otra parte, siete de las ocho **bibliotecas universitarias privadas** que contestaron a la encuesta respondieron negativamente. Sólo una contestó afirmativamente, sumando que las políticas de privacidad se encuentran a disposición del usuario, se notifica de las actualizaciones y, respecto de la frecuencia de actualizaciones responde: “siempre”.

4.3.2. Dimensión Datos

VARIABLE	PREGUNTA/S
TIPOS DE DATOS	**4. ¿Qué tipos de datos les solicita la biblioteca a los usuarios para prestar sus servicios? (Ejemplos: nombre y apellido, DNI, N° de legajo, sexo, ocupación, carrera, etc.) Especificar.**

Gráfico 1: Tipos de datos



Fuente: elaboración propia.

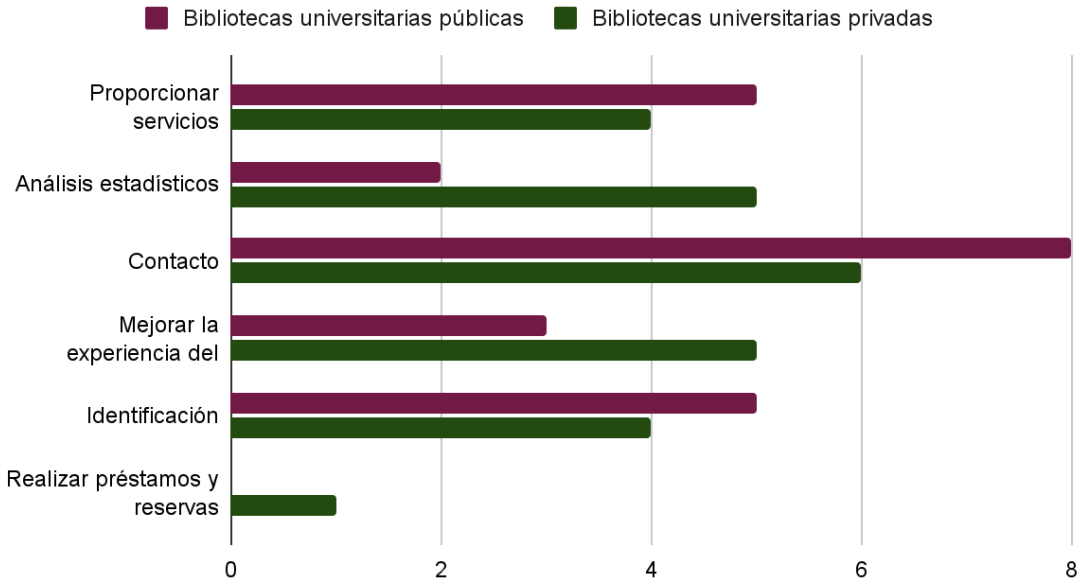
Como es posible observar, las **bibliotecas universitarias públicas** señalaron que los cuatro datos personales solicitados con mayor frecuencia son: el número de DNI, carrera que cursan los estudiantes, domicilio y su nombre y apellido. Una de las

unidades de informacion consultadas, aclaró que: “Los datos son provistos por el departamento de alumnos a través de una importación de los mismos al sistema de la Biblioteca: apellido, nombre, DNI, mail, legajo, sexo y carrera” (*).

Además, los datos personales que son solicitados con mayor frecuencia por las **bibliotecas universitarias privadas** son, el número de DNI, nombre y apellido, correo electrónico, domicilio, teléfono y carrera. Dos instituciones aclararon que: “Los datos no son solicitados por la Biblioteca” (**). “Los datos que se toman de manera automática proceden de la Base de datos de la institución” (***).

VARIABLE	PREGUNTA/S
UTILIDAD DE LOS DATOS	**5. ¿Con qué fines se registran los datos personales de los usuarios? (Puede seleccionar más de uno)** **Selecciona todos los que correspondan.** ● Proporcionar servicios ● Análisis estadísticos ● Contacto ● Mejorar la experiencia del usuario ● Identificación ● Otro

Gráfico 2: utilidad de los datos



Fuente: elaboración propia.

Según las respuestas obtenidas, en las **bibliotecas universitarias públicas**, los objetivos más comunes al registrar información personal de los usuarios son: "Contacto", "Proporcionar servicios" e "Identificación". Por otro lado, en las **bibliotecas universitarias privadas**, los datos registrados con mayor frecuencia tienen como propósito "Contacto", "Análisis estadísticos", "Mejorar la experiencia del usuario" y "Proporcionar servicios".

VARIABLE	PREGUNTA/S
CONSERVACIÓN Y ELIMINACIÓN DE LOS DATOS	**6. La base de datos en donde se almacena la información de los usuarios, ¿está incluida en el Registro Nacional de Bases de Datos (RNBD)?** ● Sí ● No **7. ¿En qué circunstancias la biblioteca decide eliminar los datos personales de un usuario? Especificar.** **8. ¿La biblioteca almacena información respecto al historial de préstamos y devoluciones de los usuarios?** ● Sí ● No **9. ¿Con qué frecuencia se elimina el historial de préstamo de los usuarios?** ● Nunca ● Rara vez ● A veces ● Casi siempre ● Siempre **10. En su biblioteca, ¿han ocurrido situaciones de riesgo que puedan haber resultado en la divulgación de datos personales de los usuarios? (Ejemplos: el acceso no autorizado a registros de usuarios, pérdida**

	o robo de dispositivos que contengan datos sensibles de los usuarios, ciberataques, etc.) ● Sí ● No

En relación con la pregunta 6, el 87,5% (siete) de las **bibliotecas universitarias públicas** respondieron negativamente, mientras que solo el 12,5% (una) lo hizo afirmativamente. Estas mismas proporciones se reflejan en las respuestas de las **bibliotecas universitarias privadas**.

Más adelante, sobre la pregunta 7, dos **bibliotecas universitarias públicas** mencionan que eliminan los datos personales cuando el usuario finaliza la carrera. Otras dos responden "nunca" y "no eliminamos los datos". Otra señala que los datos se eliminan en caso de "baja de usuario", y una más refiere que solo se eliminan "en caso de fallecimiento". Asimismo, dos instituciones proporcionan una explicación más extensa, detallando que:

- **BFdeCE**: “los datos no se eliminan porque a pesar de que egrese, para la facultad un alumno siempre es un alumno, aunque cambia a, por ejemplo, docente. Se ocultan para su uso”.

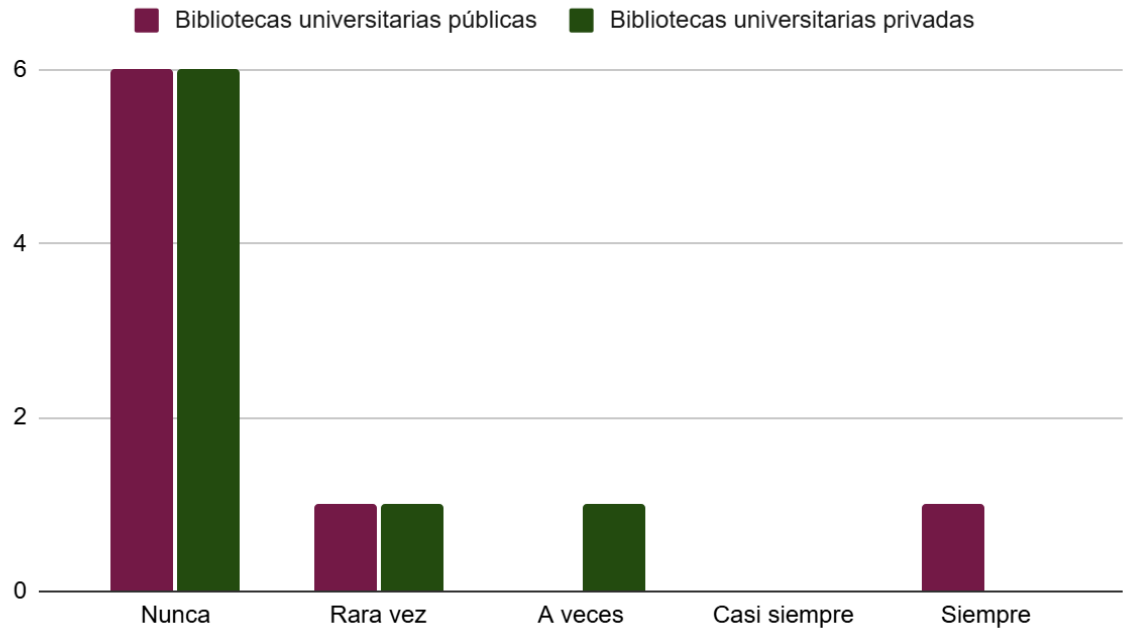
- **B"DOMC"**: “no se realiza eliminación de datos de manera selectiva por parte de la Biblioteca. La base de datos de los usuarios es compartida por todo el sistema de bibliotecas de la Universidad y la gestión técnica de la misma es centralizada. Se han realizado 'limpieza de datos' en función del estado activo o inactivo de los usuarios. Si bien podemos realizar eliminación de datos de manera individual, por el momento no tenemos una política de enfoque en la eliminación de datos (salvo casos particulares de duplicación de datos de usuarios), la misma queda en manos de los gestores técnicos del sistema”.

En respuesta a la misma pregunta, tres **bibliotecas universitarias privadas** mencionan que: “por el momento nunca eliminamos ningún dato” (**BUFASTA**), “no lo hemos hecho” (**BCODL**) y “no se eliminan” **(B “MDM”)**. Otra señala que los datos personales se descartan “cuando egresa” (**SR**) el alumno. Otra contestó que los datos se eliminan ante “baja o abandono” (**BUdelaCdelP**), y de manera similar, pero ampliando detalles, tres bibliotecas responden lo siguiente:

- **BSC**: “los datos del estudiante dejan de formar parte de la Base de datos de la que se provee la Biblioteca cuando el mismo deja de ser alumno regular, se da de baja de la matrícula o bien se gradúa.”
- **BEIM**: “cuando deja de ser alumno o docente” y “cuando vence el plazo de asociación (vecinos de la localidad)”.
- **BC**: “ante solicitud del interesado, sin embargo, no ha ocurrido”.

En la siguiente pregunta, “**8. ¿La biblioteca almacena información respecto al historial de préstamos y devoluciones de los usuarios?**”, el 87,5% (siete) de las **bibliotecas universitarias públicas** afirmaron que almacenan datos relativos al historial de préstamos y devoluciones de sus usuarios, mientras que el 12, 5% (una) estableció que no ejecuta dichos procedimientos. A su vez, las ocho **unidades de información pertenecientes a universidades privadas** que participaron de esta encuesta afirmaron que almacenan datos relativos al historial de préstamos y devoluciones de sus usuarios.

Gráfico 3: Conservación y eliminación de los datos



Fuente: elaboración propia.

Respecto a la pregunta “**9. ¿Con qué frecuencia se elimina el historial de préstamo de los usuarios?**”, fue posible recoger las siguientes respuestas entre las

bibliotecas universitarias públicas: seis determinaron que “nunca” eliminan el historial de préstamo de sus usuarios, una estableció que “rara vez” lo hacen y otra expresó que “siempre” realizan esta acción. Por otra parte, en el caso de las **bibliotecas universitarias privadas,** seis de las ocho encuestadas determinaron que “nunca” eliminan el historial de préstamo de sus usuarios, una estableció que “rara vez” lo hacen y otra expresó que “a veces” realizan esta acción.

En relación a la pregunta **“10. En su biblioteca, ¿han ocurrido situaciones de riesgo que puedan haber resultado en la divulgación de datos personales de los usuarios? (Ejemplos: el acceso no autorizado a registros de usuarios, pérdida o robo de dispositivos que contengan datos sensibles de los usuarios, ciberataques, etc.)**”, ninguna biblioteca expresó haber sufrido situaciones de riesgo que puedan haber resultado en la divulgación de datos personales de los usuarios.

4.3.3. Dimensión Usuarios

VARIABLE	PREGUNTA/S
DERECHOS DE LOS USUARIOS	**11. ¿Se le notifica al usuario respecto de los derechos que tiene sobre la información proporcionada a la biblioteca, según la Ley 25.326 de Protección de los Datos Personales?** ● Sí ● No **12. En caso de que su respuesta sea afirmativa, especificar qué información se les proporciona.** **13. ¿Se les permite a los usuarios acceder, actualizar o suprimir los datos personales que constan en la biblioteca?** ● Sí ● No **14. En caso de que haya existido o exista una situación de riesgo por la que se divulgue información de identificación personal de los usuarios, ¿se les notifica esta situación?**

	● Sí ● No

Respecto a la pregunta 11, el 75% (seis) de las **bibliotecas universitarias públicas** respondieron negativamente y el 25% (dos) afirmativamente. Por otro lado, las ocho **unidades de información de universidades privadas** que participaron en la encuesta indicaron que no notifican a sus usuarios sobre los derechos que tienen respecto a su información personal, almacenada en la unidad de información, conforme a la Ley 25.326 de Protección de los Datos Personales. Debido a que todas sus respuestas fueron negativas, no se obtuvieron devoluciones para la pregunta siguiente.

En cuanto a las dos **bibliotecas universitarias públicas** que respondieron afirmativamente, esto fue lo que expresaron en la pregunta 12:

- **BFdeCE**: “El Departamento de Alumnos realiza esta notificación en el momento de la inscripción a la facultad y a cada una de las materias. Desconozco específicamente la información que se les proporciona”.
- **BC “PAS”**: “Solo se notifica sobre el contacto de correo electrónico”.

En respuesta a la pregunta 13, el 50% (cuatro) de las **bibliotecas universitarias públicas** indicaron que sí permiten a los usuarios acceder, actualizar o suprimir sus datos personales, mientras que el otro 50% (cuatro) señaló que no permiten estos procedimientos. Estas proporciones se repiten en la información brindada por las **bibliotecas universitarias privadas** para este interrogante.

En relación con la pregunta 14, **las bibliotecas universitarias públicas** respondieron de la siguiente manera: el 62,5% (cinco) indicó que no notificaría a sus usuarios en caso de una situación de riesgo que implique la divulgación de información de identificación personal, mientras que el 37,5% (tres) afirmó que sí lo haría. Por otro lado, de las ocho **bibliotecas universitarias privadas** consultadas, el 87,5% (siete) indicó que sí avisaría a sus usuarios en tales circunstancias, y solo el 12,5% (una) señaló que no lo realizaría.

VARIABLE	PREGUNTA/S
CONSENTIMIENTO	**15. ¿Se les solicita a los usuarios la firma de un consentimiento para el uso de sus datos personales?** ● Sí ● No

En cuanto a la solicitud de consentimiento para el uso de datos personales, tanto el 87,5% (catorce) de las **bibliotecas universitarias públicas** como el mismo porcentaje de las **privadas** respondieron que no requieren la firma de un consentimiento. Solo el 12,5% (dos) de ambas afirmaron que sí solicitan a sus usuarios la firma de un consentimiento.

4.3.4. Dimensión SIGB y servicios web

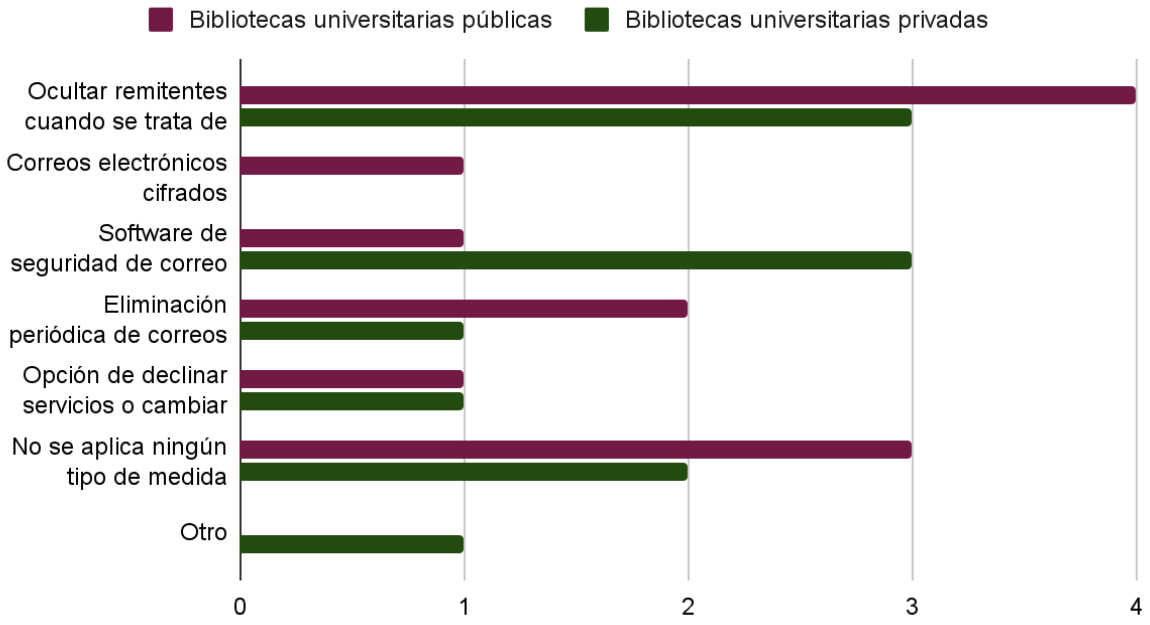
VARIABLE	PREGUNTA/S
SIGB	**16. A la hora de implementar el SIGB que utiliza la biblioteca, ¿se tuvieron en cuenta las políticas de privacidad ofrecidas por dicho software?** ● Sí ● No

A la pregunta 16, el 75% (seis) de las **bibliotecas universitarias públicas** y el 62,5% (cinco) de las **privadas** consideraron las políticas de privacidad del SIGB al implementarlo en la unidad de información. Sin embargo, el 25% (dos) de las **públicas** y el 37,5% (tres) de las **privadas** no evaluaron estas condiciones.

VARIABLE	PREGUNTA/S
CORREO ELECTRÓNICO	**17. ¿Qué medidas de protección de datos personales implementa la biblioteca al momento de enviar correos electrónicos?** ● Ocultar remitentes cuando se trata de correos electrónicos masivos.

	• Correos electrónicos cifrados. • Software de seguridad de correo electrónico. • Eliminación periódica de correos electrónicos. • Opción de declinar servicios o cambiar dirección de correo electrónico. • No se aplica ningún tipo de medida. • Otro

Gráfico 4: Correo electrónico



Fuente: elaboración propia.

En las **bibliotecas universitarias públicas** encuestadas, las tres medidas más seleccionadas fueron: "ocultar remitentes en correos masivos", "no aplicar ninguna medida" y "eliminación periódica de correos". Por otro lado, en las **privadas**, las opciones preferidas fueron: "ocultar remitentes en correos masivos", "software de seguridad para correos electrónicos" y "no aplicar ninguna medida". Además, una **biblioteca universitaria privada** eligió la opción "otro", especificando que "los correos están dentro del dominio de la universidad" (BCODL).

VARIABLE	PREGUNTA/S
REDES SOCIALES	**18. ¿Su biblioteca utiliza redes sociales para proveer o informar sobre servicios?** ● Sí ● No **19. En caso de que la respuesta anterior haya sido afirmativa, ¿se implementa algún protocolo de uso de redes sociales que involucre la protección de los datos personales de los usuarios? Especificar.**

En cuanto al uso de redes sociales, el 87,5% (siete) de las **bibliotecas universitarias públicas** y el 62,5% (cinco) de las **privadas** afirmaron utilizarlas para proveer o informar sobre servicios, mientras que el 12,5% (una) de las **públicas** y el 37,5% (tres) de las **privadas** indicaron no usar estas herramientas.

Asimismo, en respuesta a la pregunta 19, dos de las siete **unidades de información públicas** que habían respondido afirmativamente a la pregunta anterior expresaron que no implementan protocolos de uso de redes sociales que involucren la PDP de los usuarios. Las demás detallaron lo siguiente:

- **BFdeCEyE:** "no, la red social se utiliza solo para informar servicios y actividades".
- **B "DOMC":** "no hay una política de la biblioteca diseñada para tal fin. Por defecto no hacemos públicos datos personales de nuestros usuarios".
- **BC “PAS”:** "sí, del protocolo establecido por la Universidad"
- **BC “PÍJLM”:** "existen protocolos institucionales, normas de uso de las redes orientados al comportamiento e interacción, no involucran la PDP".
- **BFdeFH:** "se solicita a los usuarios consentimiento verbal para publicar las fotos".

Por su parte, las **bibliotecas privadas** que utilizan redes sociales ofrecieron las siguientes respuestas:

- **BUFASTA:** “no mostramos datos de ningún usuario y tampoco los seguimos en sus redes personales”.
- **BCODL:** “solo canalizamos información de difusión de la biblioteca”.
- **B “MDM”:** “las redes sociales se usan para informar servicios o nuevas adquisiciones. No se dan datos de usuarios. Ni fotos de ellos”.
- **BUdelaCdelP:** “reglamento”.
- **B “EIM”:** “no”.

VARIABLE	PREGUNTA/S
ACUERDOS CON TERCEROS	**20. ¿La biblioteca tiene acuerdos con terceros, tales como colaboración con otras bibliotecas, préstamo interbibliotecario, proveedores de bases de datos, revistas académicas, empresas de tecnología, etc.?** ● Sí___Continua a la pregunta 20.1. ● No__Continua a la pregunta 21 **20.1. ¿Se transfieren datos personales a terceros a la hora de efectuar una consulta que involucre a los usuarios?** ● Sí ● No **20.2. Si la respuesta anterior fue afirmativa: ¿Los datos personales de los usuarios son anonimizados antes de ser transferidos a terceros?** ● Sí___Continua a la pregunta 21 ● No___Continua a la pregunta 21

Consultados respecto a si tienen acuerdos con terceros, tanto el 87,5% (siete) de las **bibliotecas universitarias públicas** como el mismo porcentaje de las **privadas** afirmaron poseerlos, mientras que el 12,5% (una) de ambas contestó negativamente.

En respuesta a la pregunta 20.1 sobre la transferencia de datos personales a terceros, entre las bibliotecas que tienen acuerdos, el 85,7% (siete) de las **públicas**

y el 71,4% (cinco) de las **privadas** indicaron que no comparten datos personales de los usuarios al realizar consultas, mientras que el 14,3% (una) de las **públicas** y el 28,6% (dos) de las **privadas** confirmaron que sí lo hacen.

Respecto a la anonimización de datos antes de su transferencia, la **biblioteca pública** que expresó compartir datos informó que la información de los usuarios es anonimizada previamente. En contraste, de las dos **bibliotecas privadas** que transfieren datos, una indicó que no realiza la anonimización, mientras que la otra sí aplica este procedimiento antes de la transferencia.

4.3.5. Dimensión formación de usuarios y del personal bibliotecario

VARIABLE	PREGUNTA/S
FORMACIÓN DE USUARIOS	**21. Desde la biblioteca, ¿se brindan capacitaciones destinadas a usuarios sobre la protección de datos personales?** ● Sí ● No

En relación a la formación de usuarios sobre la protección de datos personales, el 87,5% (siete) de las **bibliotecas universitarias públicas** encuestadas respondió que no se realizan este tipo de actividades, mientras que el 12,5% (una) señaló que sí se llevan a cabo. Las mismas proporciones se replicaron en las respuestas aportadas por las **bibliotecas universitarias privadas**.

VARIABLE	PREGUNTA/S
CAPACITACIÓN PROFESIONAL	**22. ¿El personal bibliotecario ha recibido capacitación respecto a protección de datos personales?** ● Sí ● No

Finalmente, en cuanto a la capacitación del personal bibliotecario respecto a protección de datos personales, el 75% (seis) de las **bibliotecas universitarias públicas** encuestadas respondió que no se ha proporcionado dicha formación, mientras que el 25% (dos) indicó que sí se ha capacitado al personal en este tema.

De igual manera, en las **bibliotecas universitarias privadas**, el 75% (seis) señaló que no se ha ofrecido capacitación sobre PDP, y el 25% (dos) confirmó que su personal ha recibido esta formación.

4.4. Interpretación de los datos

Ya presentados los datos recabados, a continuación, su interpretación, teniendo en cuenta los objetivos particulares propuestos para esta tesina y las dimensiones y variables con las que se construyó la encuesta.

Atendiendo a los objetivos particulares, el desarrollo de este apartado se construye comparando el tratamiento y protección de datos personales de usuarios entre las bibliotecas universitarias públicas y privadas consultadas. A través de este procedimiento, se busca evaluar los reglamentos y políticas de privacidad de dichas bibliotecas en Argentina, con el fin de determinar en qué medida contemplan acciones que garanticen el cumplimiento de la Ley 25.326/00. Además, se pretende describir los tipos de datos personales que solicitan a sus usuarios y el tratamiento que se les da en el marco de los servicios web. También se releva la capacitación del personal bibliotecario en cuanto a estrategias de protección de datos personales.

En relación con esta legislación, tal como se mencionó en el capítulo 1 de la presente tesina, su alcance es amplio y ofrece una protección integral de los datos personales vinculados a registros, archivos y bases de datos. Por lo tanto, constituye el marco regulatorio que debe regir en todos los espacios donde se recolectan, procesan y utilizan estos datos, incluidas las unidades de información pertenecientes a instituciones universitarias.

Sin embargo, y ya iniciando con la interpretación de los datos recabados, en la **dimensión normativa**, variable marco legal, tanto bibliotecas públicas como privadas, en su mayoría coinciden en que no se menciona la Ley 25.326/00 en los documentos oficiales de las bibliotecas. En minoría responden que se registra en los reglamentos administrativos generales de la universidad que las contiene. Ya quedó establecida la relevancia de esta legislación, en el capítulo 1, al mencionar que, las garantías expresadas apuntan a proteger la intimidad y el derecho de las personas al acceso a su información personal, alojada en bases datos públicas o privadas.

En lo que respecta a la variable de políticas de privacidad, esta adquiere centralidad en la investigación. Es fundamental determinar si las bibliotecas cuentan con políticas de privacidad diseñadas específicamente por ellas, si estas se encuentran disponibles para los usuarios, si se actualizan según sus necesidades y si se informa a los usuarios sobre dichas actualizaciones. Dado que, de ser así, las unidades de información, tanto públicas como privadas, estarían explicitando la normativa vigente a través de estrategias propias. Sin embargo, ninguna de las bibliotecas universitarias públicas analizadas responde afirmativamente a estas preguntas. En el caso de las unidades de información privadas, se observa una tendencia semejante, salvo en el caso de una única biblioteca que afirma tenerlas. Por lo tanto, se puede inferir que, tanto en esta variable como en la anterior, las unidades de información de instituciones públicas y privadas se encuentran, en general, en condiciones similares.

Avanzando hacia la **dimensión datos**, variable tipos de datos, mientras que las bibliotecas públicas consultadas solicitan datos básicos como apellido y nombre, DNI, domicilio, carrera; las bibliotecas privadas amplían la solicitud con datos virtuales. Cabe aclarar aquí que, en algunos casos, los datos provienen de otras áreas administrativas de la universidad, como el departamento de alumnos, base de datos de la institución, entre otras. Asimismo, en ninguna oportunidad las unidades de información declararon recolectar datos que, según la Ley 25.326 son considerados sensibles.

Es significativo advertir la necesidad de alcanzar mejoras en cuanto a la especificidad en la recopilación y uso de los datos, como una estrategia de PDP que debe verse reflejada mediante una documentación propia. Y así, puede citarse como caso ejemplar, a la Biblioteca Digital de la Universidad de California (pública) -presentada en el capítulo 3-, que explicita sus políticas y directrices en cuanto a lo que PDP corresponde y para esto posee una Declaración de privacidad, actualizada a abril de 2024. En este documento se establece que los datos que se recopilan son información personal del usuario y por esto deben ser relevantes y necesarios para brindar servicios al público, cumplimentando las obligaciones según la ley en vigencia. Inmediatamente, la Declaración de privacidad, informa sobre qué tipo de información personal es la que se recopila. Ésta incluye la información que proporciona el usuario y la que se adquiere automáticamente.

Por su parte, la Biblioteca del Instituto Tecnológico de Massachusetts -privada, siglas en inglés *MIT*-, cuya política de seguridad de datos de los usuarios se actualizó en 2020, asume el compromiso de proteger la privacidad y confidencialidad de las personas, detallando cómo se manejan los datos personales de todos los usuarios y el marco legal que la contiene. Y aquí lo novedoso, se plantea en lo que sigue, ya tratado en extenso en el capítulo 3. La biblioteca propone como estrategia de protección una clasificación en el tipo de datos, esto es, datos de bajo riesgo, alto riesgo y riesgo medio. La distancia entre unos y otros está dada por la calidad del dato brindado, ya sea éste, uno cuya divulgación no sería perjudicial para el usuario, hasta los datos que pueden estar vinculados a requisitos de tipo legales, de índole financiera u operativos.

Continuando con el análisis de la **dimensión datos**, al avanzar hacia la variable utilidad de los datos, mientras que en las bibliotecas públicas se centra en el contacto con el usuario; en las privadas se amplía hacia la mejora del servicio proporcionado.

Asimismo, en cuanto a conservación y eliminación de los datos, como variable de análisis, el RNBD se torna relevante al ser el medio idóneo para registrar las bases de datos en los que se almacena la información de los usuarios. Cabe destacar que sólo una biblioteca pública y una privada de las encuestadas, optan por este medio. Esto coincide con lo ya manifestado en el apartado 1.3.1 del capítulo 1, donde se hace referencia a que, como resultado de una investigación, unas pocas universidades nacionales tienen debidamente inscriptas sus bases de datos. En cuanto a la encuesta realizada, el 50% de las bibliotecas públicas y el mismo porcentaje en privadas, permiten a sus usuarios acceder, actualizar o suprimir los datos personales que constan en la biblioteca. Por esto, a medida que se avanza en el análisis de las respuestas recibidas, se acentúa la necesidad de adecuar el tratamiento de los datos personales para cumplir con lo establecido por la Ley 25.326.

En cuanto al almacenamiento y/o eliminación de los datos de los usuarios, tanto bibliotecas públicas como privadas, concuerdan en sus respuestas en que depende del estado activo/inactivo del usuario; pero que, generalmente, no se eliminan ni los datos personales, ni el historial de préstamos y devoluciones. Una

sola biblioteca privada responde que pueden hacerlo ante la solicitud del usuario, aunque no tienen antecedentes hasta la fecha. Si bien la eliminación de datos está contemplada en todos los documentos analizados en el capítulo 3, cabe destacar una similitud respecto de la última respuesta presentada con la Biblioteca Central UNAM. La misma expresa que el usuario tiene derecho a solicitar la corrección de su información personal en caso de que esté desactualizada, sea inexacta o incompleta; así como de su eliminación.

Particularmente, en el caso de la eliminación de los historiales de préstamos y devoluciones, la mayoría de las bibliotecas universitarias, tanto públicas como privadas, sostienen que "nunca" descartan dicha información. Esto puede ser perjudicial, ya que -tal como se mencionó en el capítulo 1- aunque estos datos no se consideran "sensibles" según la definición legal, es importante destacar que, al combinarlos con los datos personales registrados en la biblioteca, se puede obtener información que revele los intereses o de cuenta del perfil ideológico de los usuarios (Lencinas, 2004). Esto puede ser riesgoso en situaciones donde se comprometa la seguridad informática de la unidad de información.

Avanzando hacia la **dimensión usuarios**, en la variable derechos de los usuarios, se puede realizar una comparación detallada entre las bibliotecas públicas y privadas encuestadas. En efecto, en las primeras solo dos respondieron que notifican al usuario respecto de sus derechos, de acuerdo a la ley vigente. Sin embargo, no se logra establecer con claridad qué información se les proporciona; más bien, las respuestas apelan al modo en que se realiza. Posiblemente esto sería diferente de existir un protocolo de PDP donde estén prefijados los acuerdos con los usuarios. Entre las bibliotecas privadas, ninguna informa a los usuarios acerca de sus derechos.

Lo expuesto sobre las competencias de los usuarios, puede vincularse con otra pregunta realizada, casi finalizando la encuesta. En el marco de la **dimensión formación de usuarios y del personal bibliotecario**, se consulta en la variable formación de usuarios, acerca de capacitaciones destinadas a poner en conocimiento a aquellos sobre la PDP. En todos los casos, solo una pública y una privada respondieron afirmativamente. Esto confirma, de alguna manera, la escasa relevancia que se le otorga a la información y capacitación del usuario en materia de

protección de su información personal. A lo largo del capítulo 3, este aspecto se manifiesta como altamente significativo. Tal es así que, de acuerdo a lo expresado en el apartado 3.4.1, la Biblioteca de la Universidad de Cantabria -pública- cuenta con un documento específico para la actividad de la unidad de información en lo que a PDP se refiere, actualizado en 2023, al que se le suma un informe adicional con novedosas contribuciones en cuanto a la formación del público al que atiende.

Teniendo en cuenta que, como se viene sosteniendo a lo largo de esta tesina, la protección integral de los datos personales se percibe bajo riesgo por el avance de las tecnologías y servicios que requieren proporcionar información personal, almacenada en archivos o bancos de datos, pudiendo ser objeto de uso indebido, se consulta a las bibliotecas seleccionadas acerca de, si se les notificaría a los usuarios en caso de existir una situación de riesgo en la que se divulguen sus datos de identificación personal. Y aquí surge otra oportunidad para analizar, comparativamente en detalle las respuestas recibidas.

Ante el interrogante: en caso de que haya existido o exista una situación de riesgo por la que se divulgue información de identificación personal de los usuarios, ¿se les notifica esta situación?, más del 50% de las bibliotecas públicas respondieron que no lo harían; en las privadas más del 80% respondió afirmativamente. Esta disparidad en las respuestas permite arriesgar las siguientes interpretaciones: si se ha llegado a naturalizar la idea de que los riesgos son de menor gravedad o incluso inexistentes, es comprensible que no se considere necesario informar a los usuarios. Por otro lado, cabe preguntarse si las bibliotecas privadas reconocen de manera más explícita los posibles riesgos, o si simplemente están en alerta ante la posibilidad de exponer a sus usuarios.

Al revisar los actos de protección descritos en los documentos de las bibliotecas analizadas en el capítulo 3, que se basan en las probabilidades y amenazas que pueden representar diversos riesgos, se encuentra una conexión con la Ley 25.326 vigente en Argentina. Estas amenazas afectan tanto los derechos del usuario como sus libertades. En este sentido, las acciones en torno a la seguridad y protección de los datos personales se alinean con los criterios de privacidad establecidos en las distintas políticas presentadas en el capítulo anterior, aplicando

un enfoque integral para mitigar los riesgos potenciales, tal como lo establece la Ley de Hábeas Data.

Para finalizar el análisis de la **dimensión usuarios**, resta abordar la variable del consentimiento, en donde se observa una situación de paridad, ya que el 87,5% de las bibliotecas universitarias públicas y privadas no les solicitan el consentimiento a sus usuarios para emplear sus datos, mientras que el 12,5% de ambas, sí lo hace. Ahora bien, de acuerdo con el artículo 5 de la ley vigente en la República Argentina, abordado en el capítulo 1, el tratamiento de datos personales es ilícito si el titular no ha otorgado su consentimiento libre, expreso e informado.

Sin embargo, la legislación también establece excepciones en las que no es necesario solicitar dicho consentimiento, por ejemplo, cuando los datos recolectados se limitan a nombre, DNI, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio. Aunque la mayoría de los datos requeridos por las bibliotecas encuestadas entran dentro de estas categorías, también se recolecta información adicional, como la carrera que cursan los estudiantes, correo electrónico y teléfono. Esto pone en evidencia que la mayoría de las unidades de información encuestadas no cumplen con lo dispuesto por la Ley de Hábeas Data en cuanto a la solicitud de consentimiento.

Ingresando al análisis de la **dimensión SIGB y servicios web**, se inicia con la implementación del SIGB y las políticas de privacidad ofrecidas por este software. Tanto en las bibliotecas universitarias públicas como privadas consultadas, la mayoría toman en cuenta las políticas del servicio brindado. En lo referido a la variante Correo electrónico y su uso implementando PDP, coinciden las unidades de información relevadas en, al menos un aspecto importante: se oculta el remitente cuando se trata de correos electrónicos masivos. Mientras que en la variable redes sociales, son las bibliotecas universitarias públicas las que más las utilizan, en comparación con las privadas. Sin embargo, no manifiestan -en ninguno de los dos casos-, poseer una política diseñada por la biblioteca para tal fin. Si bien concuerdan en que sólo se emplean para enviar información del servicio que brindan, el reglamento que se sigue corresponde a la universidad que las contiene.

Aparece como relevante citar aquí, ante las respuestas recibidas, lo ya desarrollado en el capítulo 3, al señalar las estrategias de la Biblioteca Central

UNAM, en cuanto a servicios web, como novedoso respecto de otros documentos similares a los analizados en ese capítulo. Se mencionan las webs *beacons*; técnicas que son utilizadas por la biblioteca para registrar la actividad del usuario en cuanto al acceso a cierto tipo de información dentro del sitio web con propósitos estadísticos y de mejora del sitio. Este registro de actividad del usuario, no se encuentra presente en otros documentos sobre privacidad de PDP analizados, pero de hecho puede ser una excelente iniciativa para incluir dentro de las estrategias de protección de datos cuando de servicios web se trata.

Ahora bien, al llegar a este punto, la variable acuerdos con terceros amerita un análisis detallado en cuanto al tratamiento y uso realizado por bibliotecas universitarias públicas y privadas a la hora de brindar servicios web. Esto es así dado que, en el capítulo 1 de esta investigación, se hace referencia al artículo 11 y 25 de la Ley de Hábeas Data, que establecen que los datos personales sólo pueden ser cedidos a terceros a fin de cumplir con el propósito de tratamiento de los datos y luego deben ser eliminados. De allí su importancia, dado que en el ámbito bibliotecario son numerosos éste tipo de procedimientos, tales como préstamo interbibliotecario, servicios comerciales para consulta de colecciones electrónicas, suscripciones a publicaciones periódicas, colaboraciones con empresas de tecnología, proveedores de SIGB, entre otros. En función de esto, se torna imprescindible la necesidad de disociar los datos personales de sus titulares o requerirles consentimiento a los usuarios de la biblioteca para su transferencia y procesamiento por parte de terceros.

A esto puede agregarse que tal y como se mencionó en el capítulo 2, la evolución de la preocupación de la ALA -Asociación de Bibliotecas de Estados Unidos-, desde hace más de tres décadas respecto a la protección de datos personales se ha mantenido en constante movimiento, de acuerdo a los desafíos que presenta el contexto histórico. Las emergencias más recientes se relacionan al uso de los datos personales como una mercancía en el mundo digital. Y en este marco, los acuerdos con terceros se tornan relevantes.

La mayoría de las bibliotecas encuestadas indicaron que tienen acuerdos con terceros, pero no transfieren datos personales de los usuarios. Sin embargo, una biblioteca universitaria pública respondió que sí los transfiere, aunque aclaró que los

datos son anonimizados previamente. De manera similar, una de las bibliotecas privadas señaló que sigue este mismo procedimiento, mientras que otra informó que transfiere los datos sin realizar su anonimización.

Si bien la relevancia de la PDP en cuanto a acuerdos con terceros, deposita en los responsables de la unidad de información la garantía de privacidad y protección de la información que se comparte de los usuarios, cabe aquí volver a traer lo presentado en el capítulo 3, referido a esta temática. En efecto, la Biblioteca de la Universidad Alfonso X el Sabio -privada- de España que, en junio de 2021, actualiza su Política de Privacidad, realiza un aporte más a lo aquí expuesto, cuando se mencionan los acuerdos con terceros, aclaran que, los datos personales pueden ser accesibles tanto a proveedores como prestadores de servicios externos. De este modo, quienes ocupan el lugar de encargados del tratamiento de los datos, son ya los terceros que, según se ratifica, están obligados por contrato a seguir los lineamientos expuestos en materia de PDP. El control de dichas acciones -que incluye inspecciones y auditorías- está a cargo de las autoridades de la universidad para comprobar en forma estricta las obligaciones legales y contractuales en materia de protección de datos personales vigentes. Esto pone de manifiesto una vez más, la relevancia que tienen las políticas de privacidad, así como las estrategias llevadas adelante por las unidades de información en cuanto a la PDP.

Así como el usuario y sus derechos ocupan un lugar central en esta tesina, no es menor el rol que desempeña el personal bibliotecario. Por esto, y dentro de la **dimensión formación de usuarios y del personal bibliotecario**, corresponde ahora analizar la variable capacitación profesional, respecto a estrategias para la PDP de los usuarios. De acuerdo a las respuestas recibidas, tanto en bibliotecas públicas como privadas, el 75% no ha recibido capacitación respecto de la PDP.

Al respecto, en el capítulo 2, ya se hizo mención a que la IFLA (2015) emite una serie de recomendaciones, entre las que se destacan: la necesidad de que las bibliotecas colaboren para proteger la privacidad y los derechos digitales contemplando la enseñanza de estrategias para garantizar la privacidad y confidencialidad en el ámbito bibliotecario como parte de la formación de los profesionales en bibliotecología. Estas recomendaciones evidencian el papel activo que deben asumir las bibliotecas y sus profesionales en estos temas. Del mismo

modo, al realizar el recorrido por el capítulo 3, el cual refiere a cada una de las bibliotecas que poseen reglamentaciones específicas para la PDP, el compromiso asumido por el personal idóneo se refleja en las estrategias implementadas, así como en el detalle de los aspectos considerados dentro de los informes, protocolos, declaraciones, entre otros, que se actualizan periódicamente para asegurar la protección y garantizar la privacidad de los usuarios de cada unidad de información citada.

Para concluir este capítulo, el análisis comparativo revela que no existen diferencias significativas en el grado de cumplimiento de la legislación vigente entre las bibliotecas universitarias públicas y privadas. Aunque se identifican algunos esfuerzos, como la revisión de las políticas de privacidad de los SIGBs al momento de implementarlos o la adopción de mecanismos básicos de protección de datos en la comunicación por correo electrónico, la realidad demuestra que ninguna de las bibliotecas encuestadas se ajusta completamente a los estándares exigidos por la Ley 25.326. Esto sugiere la necesidad de un esfuerzo conjunto para mejorar los procedimientos y prácticas relacionadas con la protección de datos en el ámbito bibliotecológico universitario del país, con el objetivo de garantizar la seguridad y privacidad de los usuarios.

En este contexto, es fundamental que las bibliotecas, sin importar su tipo de gestión, implementen estrategias claras y adecuadas para cumplir con la legislación, promoviendo la capacitación del personal, el desarrollo de políticas de privacidad propias, y el fortalecimiento de la seguridad en el manejo de los datos personales de los usuarios.

Conclusiones

A lo largo de la presente tesina se ha buscado dar respuesta al problema de investigación planteado, esto es: ¿qué estrategias implementan las bibliotecas universitarias públicas y privadas de la República Argentina para proteger los datos personales de los usuarios garantizando la aplicación de la Ley de Hábeas Data vigente?

Al llegar a este punto, puede concluirse que al analizar lo establecido por la Ley 25.326/00 de Hábeas Data, como marco normativo nacional vigente para la protección de datos personales queda claramente establecida su relevancia.

Entre los derechos personalísimos, el que refiere a la intimidad, guarda especial relación con la persona y su fuero íntimo. Por esto, el titular de este derecho cuenta con la facultad de oponerse a que su vida se vea afectada por distintas publicaciones que pueden aparecer en Internet. La divulgación de datos privados, así como de estados de su vida personal se manifiestan como más vulnerables cuando de virtualidad se trata. De allí, surge en la reforma de 1994, la incorporación del Artículo 43 con la figura del hábeas data, dentro del marco de acciones de amparo. Y, al ser incluido para proteger los derechos constitucionales, eleva –por tanto- la protección de datos personales a la categoría de derecho fundamental, tomando como base las fuentes internacionales donde se contempla este derecho.

La Ley de Hábeas Data, contiene –entre otros- los principios generales relativos a la protección de datos, los derechos de los titulares de datos, las obligaciones de responsables y usuarios de datos, el órgano de control, las sanciones y el procedimiento del recurso judicial hábeas data. Al mismo tiempo, expone los requerimientos para una protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas. Y es en este marco normativo donde se deberían inscribir las bibliotecas universitarias públicas y privadas de la República Argentina.

Al realizar un recorrido por las diferentes normas que rigen el tratamiento de datos personales en este tipo de unidades de información, se encuentra que,

ninguna de ellas cuenta con un protocolo de privacidad propio. La generalidad da cuenta que, cada una adhiere a las políticas emanadas de la universidad que las contiene. Esta ausencia implicó la necesidad de indagar en la normativa sobre PDP referida a bibliotecas universitarias en el ámbito internacional.

De este modo, se accede a las legislaciones sobre PDP en los casos de América del Norte y Europa. En este contexto, se ubican organismos supranacionales que delimitan esta temática en bibliotecas. Las normativas, aunque extensas y variadas, no presentan complejidad en su comprensión. De hecho, la Asociación de Bibliotecas de Estados Unidos, el Colegio Nacional de Bibliotecarios de México y la Federación Española de Sociedades de Archivística, Biblioteconomía, Documentación y Museística, reconocen como marco las leyes vigentes en sus países en lo referido a PDP. Luego, cada una establece, de acuerdo a la realidad de los servicios que prestan las diferentes unidades de información, protocolos y guías de protección de la privacidad de los usuarios que impactan directamente sobre las bibliotecas de Estados Unidos, México y España.

Así, los documentos analizados evidencian que el reconocimiento de los datos personales y su protección, son un derecho fundamental respaldado por organismos internacionales y, a la vez, se encuentran en el centro de la ética bibliotecaria. Las entidades y organismos comprometidos con la confidencialidad y la preservación de la privacidad de los usuarios, impulsan la toma de medidas adecuadas para evitar la divulgación no autorizada de información personal.

Ahora bien, cuando se indaga acerca del impacto que, sobre las bibliotecas universitarias de Estados Unidos, México y España tienen las normativas en vigencia, es posible acceder a declaraciones, protocolos e informes donde se advierte la preocupación por estar actualizados para garantizar la PDP de sus usuarios.

En cada una de las unidades de información seleccionadas de estos países es posible advertir la relevancia de esta temática. Con diseños accesibles, cada declaración, protocolo o informe, le indica al usuario acerca del tratamiento de los datos personales; tipos de datos y limitaciones en la recolección, uso y salvaguarda de los datos; acuerdos con terceros -en algunos casos-; derechos de los usuarios;

consentimiento informado y formación; acceso, modificación o eliminación de registros; advertencia sobre riesgos.

Al mismo tiempo, al recorrer los diferentes formatos en los que se presentan las políticas de privacidad propias de cada biblioteca, destaca la importancia atribuida al usuario como centro de las estrategias aplicadas y sujeto de formación y capacitación, para estar informado respecto a cuáles son sus derechos y cómo hacerlos cumplir. Oportunamente, se deposita en el personal bibliotecario -junto a las autoridades universitarias-, la responsabilidad para dar a conocer cada una de las decisiones que se toman en cuanto a PDP y los cambios y/o mejoras que se van introduciendo de acuerdo a las diferentes actualizaciones.

Al llegar al momento de encuestar a bibliotecas públicas y privadas argentinas en lo referido a estrategias concretas para la implementación de la Ley de Hábeas Data, evaluando reglamentos y políticas de privacidad implementadas, comparando el tratamiento y protección de datos personales solicitados a la hora de brindar servicios web e indagando en la capacitación ofrecida tanto a usuarios como al personal bibliotecario en bibliotecas universitaria públicas y privadas, los resultados ratificaron las ausencias destacadas en el estado del arte de esta tesina. Con la salvedad de los casos presentados en la UNSL y la UCC, que hacen una breve mención a la legislación anteriormente mencionada, en diferentes normativas institucionales.

De acuerdo a los resultados obtenidos en cada una de las dimensiones que se implementaron en la encuesta, en la comparación entre bibliotecas universitarias públicas y privadas realizadas en el apartado anterior, puede concluirse que, en la **dimensión normativa**, una proporción mínima -solo tres- de las unidades de información mencionan la Ley 25.326/00 en sus documentos oficiales. Tampoco se han elaborado protocolos de protección propios, a excepción de una biblioteca que sí declaró haberlo hecho. En cuanto a la **dimensión datos**, su compilación, tratamiento, modificación y/o eliminación, se realiza en forma similar; esto es, con mínimos resguardos de seguridad para el usuario. En la **dimensión usuarios**, la tendencia señala que no se les notifica acerca de sus derechos y tampoco se los forma para que puedan reclamar por el cumplimiento de la normativa vigente. Ante la presencia de posibles riesgos frente a la divulgación de datos, la disparidad en las

respuestas permitiría inferir, por un lado, la naturalización de la no existencia de peligros informáticos o que casi nunca se estaría frente a ellos y por el otro, un reconocimiento de manera más explícita los posibles riesgos y la precaución ante la posibilidad de exponer a los usuarios. Más adelante, habiendo sido confirmado como un documento importante en la responsabilidad del manejo de datos de parte del personal bibliotecario, el consentimiento del usuario no es considerado como tal en el contexto de las bibliotecas encuestadas. En cuanto a la **dimensión SIGB y servicios web**, coinciden las unidades de información relevadas en, al menos un aspecto importante; esto es, se oculta el remitente cuando se trata de correos electrónicos masivos. Sin embargo, no siempre se anonimizan los datos al momento de transferirlos a terceros. Por último, en la **dimensión formación de usuarios y del personal bibliotecario**, así como no se forma al usuario en la PDP, tampoco se capacita al personal bibliotecario, teniendo en cuenta la responsabilidad que recae sobre ellos a la hora de acumular, tratar, usar y eliminar datos personales.

En el análisis de las bibliotecas universitarias públicas y privadas que surge de la encuesta realizada, se advierte que si bien se toman ciertas medidas para la protección de datos personales de los usuarios, en ningún caso se aplican los requisitos establecidos por la Ley 25.326 de manera completa. Aunque algunas de las variables consultadas cuentan como registro dentro del marco que otorgan las políticas de privacidad de la universidad que las contiene, la especificidad propia del entorno bibliotecario continúa ausente, así como la sistematización de las estrategias que, de manera dispar, se implementan.

Teniendo en cuenta lo hasta aquí expresado, aparece como pertinente incluir -de acuerdo a los objetivos específicos planteados-, un conjunto de sugerencias destinadas a bibliotecas universitarias argentinas, a fin de promover el cumplimiento de los requisitos establecidos por la Ley de Hábeas Data. Para su elaboración se tuvieron en cuenta las pautas publicadas por la ALA (2003) para el desarrollo de políticas de privacidad en bibliotecas, la legislación nacional anteriormente mencionada y los documentos relacionados con la PDP que fueron analizados en el capítulo 3. Es importante señalar que este listado se organiza conforme a las dimensiones estipuladas en la encuesta dirigida a las unidades de información relevadas.

NORMATIVA
● Referir a la Ley 25.326 en todos los documentos oficiales de la biblioteca que involucren el tratamiento de datos personales de los usuarios. ● Elaborar políticas de privacidad específicas para la unidad de información y garantizar que sean fácilmente accesibles al público, tanto en formato físico como en la web. ● Revisar y actualizar dichas políticas de forma periódica, notificando a los usuarios sobre cualquier modificación.
DATOS
● Limitar la recopilación de información personal a lo estrictamente necesario para el funcionamiento de los servicios. ● Establecer procedimientos claros para la destrucción regular de registros que contengan datos personales, como historiales de circulación, perfiles de usuarios inactivos o datos de uso de recursos electrónicos. ● Implementar medidas técnicas y organizativas para proteger los datos personales de accesos no autorizados, pérdida o robo. ● Al realizar estadísticas, desvincular los datos que revelan la identidad de los usuarios de la información sobre el uso de los servicios bibliotecarios. ● Proporcionar al usuario un documento que detalle los tipos de datos recolectados por la biblioteca y la justificación de su solicitud, explicando su utilidad.
USUARIOS

- Informar y garantizar a los usuarios su derecho a acceder, modificar o eliminar los datos personales registrados por la biblioteca.
- Solicitar el consentimiento explícito de los usuarios para el tratamiento de sus datos personales, cuando se requiera información adicional a la siguiente lista: nombre, DNI, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio.
- Notificar a los usuarios en caso de que ocurra una situación de riesgo que pudiera comprometer la divulgación de sus datos personales, registrados en la biblioteca.

SIGB Y SERVICIOS WEB

- Registrar las bases de datos pertenecientes a la biblioteca en el RNBD.
- Ocultar remitentes de correos electrónicos masivos.
- Diseñar políticas o protocolos de privacidad exclusivos para el uso de las redes sociales de la biblioteca.
- Evaluar continuamente las políticas de privacidad de los sistemas pertenecientes a terceros con los que la biblioteca establezca acuerdos, para evitar incompatibilidades y detectar actualizaciones.
- Garantizar la anonimización de los datos personales de usuarios que son transmitidos a terceros.

FORMACIÓN DE USUARIOS Y DEL PERSONAL BIBLIOTECARIO

- Ofrecer capacitaciones regulares sobre protección de datos personales, dirigidas tanto al personal bibliotecario como a los usuarios de la unidad de información.

Las sugerencias aquí presentadas, buscan ser un aporte para la comunidad de bibliotecas universitarias argentinas, públicas y privadas, entendiendo que la protección de datos personales supone la implementación de un conjunto de medidas destinadas a garantizar el derecho a la privacidad. El cual es, a su vez, condición necesaria para ejercer los derechos al acceso libre a la información y a la libertad de expresión, pilares fundamentales del quehacer bibliotecario.

Cabe agregar que las estrategias destinadas a la protección de datos personales en bibliotecas no deben ser estáticas -de allí que las sugerencias refieren al estado actual de las bibliotecas relevadas-, ya que dependen de los cambios que puedan realizarse a nivel legislativo y de las transformaciones que ocurran en el contexto de las unidades de información. En este sentido, es fundamental que evolucionen en paralelo con las instituciones a las que pertenecen.

Para finalizar, la presente tesina apunta a visibilizar la relevancia del cumplimiento de la Ley 25.326, a la vez que reforzar el papel de las bibliotecas como espacios comprometidos con el bienestar y la formación de sus usuarios. La protección de la información de carácter personal debe ser una prioridad en la práctica diaria de las bibliotecas universitarias, a fin de crear un entorno más seguro y respetuoso con el derecho a la privacidad, donde los usuarios puedan interactuar con confianza en un mundo digital cada vez más complejo.

Referencias bibliográficas

Agüero Ovejero, I. (2019). La protección de datos frente al alto grado de libertad de la GAFA (Google, Apple, Facebook y Amazon). *Revista de Derecho, Ciencias Sociales y Políticas*, *25*, 20-28. https://revistaschilenas.uchile.cl/handle/2250/109267

Asamblea General de la ONU. (1948). Declaración Universal de los Derechos Humanos (217 [III] A). París.

Asociación de bibliotecas de los Estados Unidos. (2021). Resolution on the Misuse of Behavioral Data Surveillance in Libraries. http://www.ala.org/advocacy/intfreedom/datasurveillanceresolution

Asociación de bibliotecas de los Estados Unidos. (2017). Resolution to Protect Library User Confidentiality in Self-Serve Hold Practices. http://www.ala.org/advocacy/intfreedom/statementspols/ifresolutions/selfserveholds

Asociación de bibliotecas de los Estados Unidos. (2017). Hoja de datos sobre ALA. http://www.ala.org/aboutala/offices/hoja-de-datos-sobre-ala

Asociación de Bibliotecas de Estados Unidos. (7 de julio de 2006). Privacy: An Interpretation of the Library Bill of Rights http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy

Asociación de bibliotecas de los Estados Unidos. (2006). Library Bill of Rights. http://www.ala.org/advocacy/intfreedom/librarybill

Asociación de bibliotecas de los Estados Unidos. (2006). Policy concerning Confidentiality of Personally Identifiable Information about Library Users. http://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconcerning

Asociación de bibliotecas de los Estados Unidos. (2006). Policy on Confidentiality of Library Records.https://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconfidentiality

Asociación de bibliotecas de los Estados Unidos. (2006). Privacy: An Interpretation of the Library Bill of Rights. https://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy#Notes

Asociación de bibliotecas de los Estados Unidos. (2006). Resolution on the Retention of Library Usage Records. https://alair.ala.org/bitstream/handle/11213/1594/52.4.4%20Retention%20of%20Library%20Records.pdf?sequence=1&isAllowed=y

Asociación de bibliotecas de los Estados Unidos. (2007). State Privacy Laws Regarding Library Records. http://www.ala.org/advocacy/privacy/statelaws

Asociación de bibliotecas de los Estados Unidos. (2003). Guidelines for Developing a Library Privacy Policy. https://www.olaweb.org/assets/IntellectualFreedom/IF_Toolkit/ala_guidelines_privacypolicy.pdf

Asociación de Estados EIberoamericanos para el Desarrollo de las Bibliotecas Nacionales de los Países de Iberoamérica. (2023). La Importancia de la Privacidad y la Protección de Datos en las Bibliotecas. http://asociacionabinia.org/la-importancia-de-la-privacidad-y-la-proteccion-de-datos-en-las-bibliotecas/

Basterra, M. (2013). La garantía constitucional del Hábeas Data. Lineamientos generales de la Ley de Protección de Datos Personales. https://marcelabasterra.com.ar/wp-content/uploads/2016/11/La-Garanti%cc%81a-Constitucional-de-Habeas-Data.-Lineamientos-generales.pdf

Basterra, M. (2010). Hábeas Data: los derechos protegidos. En P. Manili, Tratado de derecho procesal constitucional. Argentino, Comparado y Trasnacional (pp. 1-28). Editorial La Ley. https://marcelabasterra.com.ar/wp-content/uploads/2016/11/HD.-Habeas-Data.-Derechos-Protegidos.-Marcela-I.-Basterra.-03.3.10.pdf

Basterra, M. (2004). El consentimiento del afectado en el proceso de tratamiento de

datos personales. https://marcelabasterra.com.ar/wp-content/uploads/2016/11/HD.-El-consentimiento-del-afectado-en-el-proceso-de-tratamiento-de-datos-personales.pdf

Biblioteca de la Comisión Económica para América Latina y el Caribe. (18 de diciembre de 2020). Gestión de datos de investigación. Sobre la protección de los datos. https://biblioguias.cepal.org/gestion-de-datos-de-investigacion

Biblioteca Central UNAM. (2022). Aviso de Privacidad Integral de la Dirección General de Bibliotecas y Servicios Digitales de Información (DGBSDI) de la Universidad Nacional Autónoma de México. https://www.bibliotecacentral.unam.mx/index.php/quienes-somos/aviso-de-privacidad/300-aviso-de-privacidad-integral-dgbsdi-unam

Biblioteca de la Universidad de Cantabria. (2023). Política de Protección de Datos Personales. Actividad de tratamiento: “Biblioteca”. https://web.unican.es/consejo-direccion/gerencia/RGDP/rgpd_info_biblioteca.pdf

Biblioteca Universitaria UAX (2021) Política de privacidad. https://biblioteca.uax.es/politica-privacidad.html

Bowers, S. (2006). Privacy and Library Records. *The Journal of Academic Librarianship*, *32*(4), 377–383. https://sci-hub.se/http://dx.doi.org/10.1016/j.acalib.2006.03.005

Buró Federal de Investigación. (s.f.). La Ley de Derechos Educativos y Privacidad Familiar (FERPA, por su sigla en inglés) Una guía para los socorristas y el personal policial. https://www.fbi.gov/file-repository/ferpa_spanish1.pdf

California Digital Library. (2024). Declaración de privacidad. University of California. https://cdlib.org/about/policies-and-guidelines/privacy-statement/#personal-information-we-colle

California Digital Library. (2024a). Políticas y directrices. University of California. https://cdlib.org/about/policies-and-guidelines/

Código de ética para bibliotecarios y profesionales de la información en España. (2013) https://www.fesabid.org/wp-content/uploads/repositorio/codigo-etico-esp.pdf

Código de Ética. Colegio Nacional de Bibliotecología. México. (2017) https://cnbmx.org/index.php/documentos/codigo-de-etica

Constitución española. 1978. https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf

Constitución Política de los Estados Unidos Mexicanos [Const]. Art. 6. 5 de febrero de 1917. (Estados Unidos Mexicanos).

Diccionario panhispánico del español jurídico. (2023). Protección de datos. https://dpej.rae.es/lema/protecci%C3%B3n-de-datos

Directiva 95/46/CE. Reglamento general de protección de datos. España. (2016) http://data.europa.eu/eli/reg/2016/679/2016-05-04

Federación Española de Sociedades de Archivística, Biblioteconomía, Documentación y Museística. (2024) https://www.fesabid.org/

Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas. (2015). Declaración de la IFLA sobre la privacidad en el Entorno Bibliotecario. https://www.ifla.org/wpcontent/uploads/2019/05/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment-es.pdf

Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas. (2012). Código de ética de la IFLA para bibliotecarios y otros trabajadores de información. https://www.ifla.org/wp-content/uploads/2019/05/assets/faife/codesofethics/spanishcodeofethicsfull.pdf

Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas. (2012). Código de ética de la IFLA para bibliotecarios y otros trabajadores de información. https://www.ifla.org/wp-content/uploads/2019/05/assets/faife/codesofethics/spanishcodeofethicsfull.pdf

Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas. (2006). Manifiesto de la IFLA sobre Internet Directrices. https://archive.ifla.org/faife/policy/iflastat/Internet-ManifestoGuidelines-es.pdf

Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas. (2002). Manifiesto de la IFLA sobre Internet. https://cdn.ifla.org/wp-content/uploads/2019/05/assets/faife/publications/policy-documents/Internet-manifesto-es.pdf

Ferreira Dos Santos, J. (2019). La privacidad en servicios de biblioteca. En Morán Guzmán, A. y López Ruelas, S. (Eds.), *Transformando Bibliotecas: privacidad y libre acceso* (pp. 41-52). Universidad de Guadalajara. https://coloquiobibliotecarios.udg.mx/sites/default/files/2022-12/transformando-bibliotecas-privacidad-y-libre-acceso_0.pdf#page=40

García González, A. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. *Boletín Mexicano de Derecho Comparado,* *40*(120),743-778. https://www.researchgate.net/publication/26549191_La_proteccion_de_datos_personales_derecho_fundamental_del_siglo_XXI_Un_estudio_comparado

Gómez Sánchez, M. (2020). La protección de datos personales en México: cambios evolutivos a 10 años de su inclusión a nivel constitucional. Revista Mexicana de Ciencias Penales, 3 (10), 48-58. https://revistaciencias.inacipe.gob.mx/index.php/02/article/view/97/98

Hernández Sampieri, R, Fernández Collado, C. y Baptista Lucio, P. (2010). Metodología de la investigación. 5° Edición. McGraw Hill, México.

Hernández Sampieri, R, Fernández Collado, C. y Baptista Lucio, P. (2014). Metodología de la investigación. 6° Edición. McGraw Hill, México. https://www.academia.edu/20792455/Metodología_de_la_Investigacion_6ta_edicion_Roberto_Hernandez_Sampieri

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2021). Normativa y legislación en PDP. Leyes en México para la

protección de datos personales. https://micrositios.inai.org.mx/marcocompetencias/?page_id=370

Kraemer, E. O. (noviembre de 2011). La ética profesional y la formación de bibliotecarios en el área de los procesos técnicos [ponencia]. VII Encuentro Internacional y III Nacional de Catalogadores, Buenos Aires, Argentina. https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.bn.gov.ar/resources/conferences/encuentroIII/ponencia-25-M-Kraemer.pdf&ved=2ahUKEwjY2aq6o-P4AhWUupUCHZuaD8sQFnoECBEQAQ&usg=AOvVaw31NGw_wYYZEcSyD4y3sZbg

Lencinas, V. (27-28 de agosto de 2004). *Algunas problemáticas relacionadas con las TIC's y la bibliotecología* [Conferencia]. 1er Foro Social de Información, Documentación y Bibliotecas, Buenos Aires, Argentina. http://eprints.rclis.org/6205/1/65.pdf

Ley de Bibliotecas de la Ciudad de México. 18 de marzo de 2020. Gaceta Oficial de la Ciudad de México. https://www.congresocdmx.gob.mx/media/documentos/f8209d5b6a1e7b8eaa8e08d9a5679548d8d16984.pdf

Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales. 6 de diciembre de 2018. Boletín Oficial No. 294. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

Ley Orgánica 15/1999. Protección de Datos de Carácter Personal. 14 de diciembre de 1999. Boletín Oficial No. 298. https://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf

Ley 10/2007, de 22 de junio, de la lectura, del libro y de las bibliotecas. 23 de junio del 2007. Boletín Oficial No. 150. https://www.boe.es/buscar/act.php?id=BOE-A-2007-12351

Ley 25326 de 2000. Protección de los Datos Personales. 30 de octubre de 2000. Boletín Oficial No. 29517. http://servicios.infoleg.gob.ar/infolegInternet/anexos/6000064999/64790/texact.htm

Martín Gavilán, C. (2009). Temas de Biblioteconomía: Servicios al usuario: accesibilidad a los documentos, préstamo y préstamo interbibliotecario. http://eprints.rclis.org/14283/1/prestamo.pdf

López Torres, J. (2014). Antecedentes internacionales en materia de privacidad y protección de datos personales. *Journal of international law*, 5(2), 103-117. https://publicaciones.eafit.edu.co/index.php/ejil/article/view/2849/2616

Masciotra, M. (2020). Protección de datos personales ante la pandemia del Coronavirus. http://www.saij.gob.ar/DACF200155

MIT Libraries. (2020). Política de privacidad de datos de usuario. https://libraries.mit.edu/about/policies/privacy-policy/

Morán, A. (2017). Dimensiones éticas de la bibliotecología: Puntos relevantes a considerar para la posibilidad de un nuevo código de ética profesional para bibliotecólogos en México.

Morán Guzmán, A. G., López Ruelas, S. (compiladores). (2019). Transformando bibliotecas: privacidad y libre acceso. Guadalajara, Jalisco: Universidad de Guadalajara. Coordinación de Bibliotecas. https://coloquiobibliotecarios.udg.mx/sites/default/files/2022-12/transformando-bibliotecas-privacidad-y-libre-acceso_0.pdf

Oficina del alto comisionado de la Naciones Unidas para los Derechos Humanos. (1988). Derecho a la intimidad (Art. 17). HRC Observación general Nº 16. https://www.acnur.org/fileadmin/Documentos/BDL/2005/3584.pdf

Proyecto de Ley sobre Reglamentación del Ejercicio Profesional en Bibliotecología y Documentación. (2005). https://www.senado.gob.ar/web/proyectos/verExpe.php?origen=S&numexp=799/05&tipo=PL&tConsulta=1

Quispe Gerónimo, C. (septiembre de 2003). *Bibliotecarios y terrorismo: principios éticos del derecho a la privacidad y el acceso a la información*. Seminario de la Realidad Bibliotecológica, Lima, Perú. https://www.researchgate.net/publication/28805554_Bibliotecarios_y_terrorismo

_principios_eticos_del_derecho_a_la_privacidad_y_el_acceso_a_la_informacion

Reggiani, F. (2006). Acceso, intimidad y propiedad: Problemas éticos y tecnología en las bibliotecas. Palabra Clave. Edición especial. 69-82. En Memoria Académica. http://www.memoria.fahce.unlp.edu.ar/art_revistas/pr.4317/pr.4317.pdf

Ramos, S. (2007). Hábeas data. Protección de datos personales. SAIJ. http://www.saij.gob.ar/santiago-jose-ramos-habeas-data-proteccion-datos-personales-dacf070031-2007/123456789-0abc-defg1300-70fcanirtcod

Saldaña, M. (2011). El derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego. *Teoría y Realidad Constitucional*, (28), 279-312.http://e-spacio.uned.es/fez/eserv/bibliuned:TeoriayRealidadConstitucional-2011-28-2070/Documento.pdf

Sistema de Bibliotecas de la Universidad Católica de Córdoba. (2024). Política de comunicación DIR-34-SB-01 https://biblioteca.ucc.edu.ar/wp-content/uploads/2020/12/Politica-de-comunicaci%C3%B3n-completa.pdf

Tamperini, M. (11 de julio de 2013). Gestión de Datos Personales en las Universidades Nacionales de Argentina. Observatorio Iberoamericano de Protección de Datos. https://oiprodat.com/2013/07/11/gestion-de-datos-personales-en-las-universidades-nacionales-de-argentina/

Universidad Alfonso X el Sabio. (2022). Datos matrícula. https://www.uax.com/noticias/la-universidad-alfonso-x-el-sabio-da-la-bienvenida-a-los-cerca-de-8.000-estudiantes-que-se-suman-este-curso-a-la-comunidad-uax

Universidad de California. (2020). Datos matrícula. https://nces.ed.gov/programs/digest/d21/tables/dt21_312.10.asp

Universidad La Salle. (2020). Política de Privacidad. https://lasalle.mx/globales/aviso-de-privacidad/tratamientos/tratamientos-administrativos-generales.html

Universidad Nacional Autónoma de México. (2022). Datos matrícula. https://www.economia.gob.mx/datamexico/es/profile/institution/universidad-nacional-autonoma-de-mexico

Universidad Nacional de San Luis. (2021). Reglamento del sistema de bibliotecas de la Universidad Nacional de San Luis. http://biblioteca.unsl.edu.ar/website/pdf/reglamento.pdf

Valesani, M., Mariño, S. y La Red, D. (2003). La protección de los datos personales en los sistemas informáticos. La instrumentación en la Argentina. *CISIC, 2*, 246-257. https://www.researchgate.net/profile/David-Red-2/publication/228718681_La_Proteccion_de_los_Datos_Personales_en_los_Sistemas_Informaticos_La_Instrumentacion_en_la_Argentina/links/00b4953437997c58f1000000/La-Proteccion-de-los-Datos-Personales-en-los-Sistemas-Informaticos-La-Instrumentacion-en-la-Argentina.pdf

Varela-Orol, C. y Ameneiros Rodríguez, R. (2018). La protección de datos personales en las bibliotecas universitarias españolas en el entorno digital. *Revista General de Información y Documentación, 28*(2), 685-702. https://revistas.ucm.es/index.php/RGID/article/view/62844

Vaughan, J. (2020). Políticas de privacidad de bibliotecas. *Library Technology Reports, 56*(6), 5-53. https://journals.ala.org/index.php/ltr/issue/view/771

Vega, G. (2022) Principios relacionados con el uso de datos personales en bibliotecas. Amontonamos las palabras: Blog de la Biblioteca de El Colegio de México. https://bdcv.hypotheses.org/4564

Venteño Jaramillo, G. y Casas Castillo, F. (2013). El levantamiento de datos estadísticos en la biblioteca. *Biblioteca Universitaria, 16*(1), 46-53. https://www.redalyc.org/pdf/285/28528266005.pdf

Witt, S. (2017). The Evolution of Privacy within the American Library Association, 1906-2002. *Library Trends*, *65*(4), 639–657. doi:10.1353/lib.2017.0022

Zimmer, M. (2014). Librarians' Attitudes Regarding Information and Internet Privacy. *The Library Quarterly*, *84*(2), 123-151. https://sci-hub.se/https://www.journals.uchicago.edu/doi/abs/10.1086/675329

Anexo

Listado de los sitios web relevados, correspondientes a 49 unidades de información universitarias, tanto públicas y privadas, ubicadas en las 23 provincias argentinas y la Ciudad Autónoma de Buenos Aires

PROVINCIA	UNIVERSIDADES NACIONALES	BIBLIOTECA	SITIO WEB
Buenos Aires	Universidad Nacional de La Plata	Biblioteca Pública Universidad Nacional de La Plata	https://www.biblio.unlp.edu.ar/
CABA	Universidad Nacional de Buenos Aires	Biblioteca “Profesor Emérito Alfredo L. Palacios”	http://biblio.economicas.uba.ar/Content/faq
Catamarca	Universidad Nacional de Catamarca	Biblioteca Central de la Universidad Nacional de Catamarca	https://www.unca.edu.ar/pagina-23-bibliotecas-99.html
Chaco	Universidad Nacional del Chaco Austral	Biblioteca Universidad Nacional del Chaco Austral	https://uncaus.edu.ar/index.php/academica/biblioteca
Chubut	Universidad Nacional de la Patagonia San Juan Bosco	Biblioteca Central Dr. Eduardo A. Musacchio	https://www.unp.edu.ar/biblioteca/
Córdoba	Universidad Nacional de Córdoba	Biblioteca «Elma Kohlmeyer de Estrabou»	https://ffyh.unc.edu.ar/biblioteca/
Corrientes	Universidad Nacional del Nordeste	Biblioteca Central «Prof. Ítalo Juan Luis Mettini»	https://bib.unne.edu.ar/biblioteca-central/
Entre Ríos	Universidad Nacional de Entre Ríos	Biblioteca Central “Prof. Antonio Serrano”	https://biblioteca-rect.uner.edu.ar/

Formosa	Universidad Nacional de Formos	Biblioteca Central “Prof. Miguel D. Ivancovich”	https://www.unf.edu.ar/biblioteca-central-unaf/
Jujuy	Universidad Nacional de Jujuy	Biblioteca "Ana María Postigo De De Bedia"	https://www.fhycs.unju.edu.ar/biblioteca.html
La Pampa	Universidad Nacional de La Pampa	Biblioteca Central	https://www.unlpam.edu.ar/biblioteca/biblioteca-central
La Rioja	Universidad Nacional de La Rioja	Biblioteca Ángel María Vargas	https://www.unlar.edu.ar/index.php/component/content/article?id=47
Misiones	Universidad Nacional de Misiones	Biblioteca de la Facultad de Humanidades y Ciencias Sociales	https://www.fhycs.unam.edu.ar/portada/biblioteca/
Mendoza	Universidad Nacional de Cuyo	Biblioteca Central «Dr. Arturo Andrés Roig»	https://sid.uncu.edu.ar/sid/biblioteca-central/
Neuquén	Universidad Nacional del Comahue	Biblioteca Central Francisco P. Moreno	https://bibliocentral.uncoma.edu.ar/
Río Negro	Universidad Nacional de Río Negro	Biblioteca Central Sede Atlántica	https://www.unrn.edu.ar/section/59/bibliotecas.html
Salta	Universidad Nacional de Salta	Biblioteca "Prof. Eusebio Cleto del Rey"	https://biblioeco.unsa.edu.ar/index.php/
San Juan	Universidad Nacional de San Juan	Biblioteca Central de la Facultad de Ciencias Sociales	https://www.facso.unsj.edu.ar/institucional/institucional/9
San Luis	Universidad Nacional de San Luis	Biblioteca Central "Antonio Esteban Agüero"	http://biblioteca.unsl.edu.ar/website/baea/baea-new.html

Santa Cruz	Universidad Nacional de la Patagonia Austral	Biblioteca Académica Malvina Perazo UNPA – UARG	https://www.uarg.unpa.edu.ar/biblioteca/
Santa Fe	Universidad Nacional de Rosario	Biblioteca "Estanislao S. Zeballos" de la Facultad de Ciencias Económicas y Estadística	https://archivo.fcecon.unr.edu.ar/web-nueva/servicios-y-organizacion
Santiago del Estero	Universidad Nacional de Santiago del Estero	Biblioteca Central de la Universidad Nacional de Santiago del Estero	http://libnet.unse.edu.ar/
Tierra del Fuego	Universidad Nacional de Tierra del Fuego, Antártida e Islas del Atlántico Sur	Biblioteca Sede Ushuaia "Ester Liva"	https://sisbi.untdf.edu.ar/cgi-bin/koha/opac-library.pl?branchcode=US
Tucumán	Universidad Nacional de Tucumán	Biblioteca Facultad de Derecho y Ciencias Sociales	http://biblioteca.derecho.unt.edu.ar/
PROVINCIA	**UNIVERSIDADES PRIVADAS**	**BIBLIOTECA**	**SITIO WEB**
Buenos Aires	Universidad FASTA	Biblioteca de la Universidad FASTA	https://www.ufasta.edu.ar/biblioteca/
	Universidad de Morón	Biblioteca Mariano Moreno	https://www.unimoron.edu.ar/area/biblioteca
CABA	Universidad Argentina de la Empresa	Biblioteca UADE	https://biblioteca.uade.edu.ar/client/es_ES/biblioteca

	Universidad Abierta Interamericana	Biblioteca Central UAI	https://biblioteca.vaneduc.edu.ar/#/
	Universidad Católica Argentina	Biblioteca San Benito Abad	https://biblioteca.uca.edu.ar/bibliotecas.html
	Universidad del Salvador	BIBLIOTECA CENTRAL "R.P. Guillermo Furlong, S.J."	https://noticias.usal.edu.ar/es/redbus
	Universidad de Belgrano	Biblioteca central	https://biblioteca.ub.edu.ar/
	UCES	Biblioteca UCES CENTRO	https://biblioteca.uces.edu.ar/biblioteca/centro
	Universidad Maimónides	Biblioteca central	https://www.maimonides.edu/biblioteca/
	Universidad de Palermo	Biblioteca Central	https://www.palermo.edu/biblioteca/
	Universidad Argentina John F. Kennedy	Biblioteca Central	https://www.kennedy.edu.ar/alumnos/biblioteca/
Córdoba	Universidad Empresarial Siglo 21	Biblioteca Campus	https://21.edu.ar/estudiantes/recursos/biblioteca
	Universidad Católica de Córdoba	Biblioteca “Dr. Gustavo Ortiz”	https://biblioteca.ucc.edu.ar/sistema-de-bibliotecas-uccb/biblioteca-ortiz/
	Universidad Blas Pascal	Biblioteca	https://www.ubp.edu.ar/biblioteca/
Corrientes	Universidad de la Cuenca del Plata	Biblioteca Universidad de la Cuenca del Plata	https://www.ucp.edu.ar/biblioteca/

Entre Ríos	Universidad Adventista del Plata	Biblioteca E. Irving Mohr	https://biblioteca.uap.edu.ar/consultas/
Misiones	Universidad Gaston Dachary	Biblioteca Central	https://ugd.edu.ar/es/106-la-universidad/39-biblioteca
Mendoza	Universidad de Mendoza	Biblioteca Sede Central	https://um.edu.ar/biblioteca/staff-biblioteca/
	Universidad de Congreso	Biblioteca “Luis Menotti Pescarmona”	https://www.ucongreso.edu.ar/alumnos/biblioteca/
Salta	Universidad Católica de Salta	Biblioteca Central	https://www.ucasal.edu.ar/menu-servicios-biblioteca-sistema-de-bibliotecas/
San Juan	Universidad Católica de Cuyo	Biblioteca “Monseñor Dr. Manfredi”	https://www.uccuyosj.edu.ar/index.php/alumnos/biblioteca-central
Santa Fe	Universidad del Gran Rosario	Sede Rosario	https://ugr.edu.ar/biblioteca-nuevo/sobre-las-bibliotecas-ugr/
Santiago del Estero	Universidad Católica de Santiago del Estero	Biblioteca Central “Orestes Di Lullo”	https://www.ucse.edu.ar/biblioteca/
Tucumán	Universidad del Norte Santo Tomás de Aquino	Biblioteca Sede Central	https://www.unsta.edu.ar/biblioteca-unsta/

Encuesta para personal bibliotecario de bibliotecas universitarias públicas y privadas seleccionadas

1. ¿La Institución en la que usted se desempeña es pública o privada?

NORMATIVA

Marco legal

2. ¿Se menciona la aplicación de la Ley 25.326 de Protección de los Datos Personales en algún documento oficial de la biblioteca (Reglamento, Manual de Procedimientos, Estatuto, Protocolo, etc.)? Especificar.

3. ¿Disponen de políticas de privacidad especialmente diseñadas por y para la biblioteca?

Sí. Continua a la pregunta 3.1.
No. Continua a la pregunta 4.

Políticas de privacidad

3.1. Estas políticas de privacidad, ¿se encuentran disponibles en la web para los usuarios?

Sí
No

3.2. ¿Con qué frecuencia se actualizan las políticas de privacidad?

Nunca
Rara vez
A veces
Casi siempre
Siempre

3.3. ¿Se notifica a los usuarios de dichas actualizaciones?

Sí. Continua a la pregunta 4
No. Continua a la pregunta 4

DATOS

Tipos de datos

4. ¿Qué tipos de datos les solicita la biblioteca a los usuarios para prestar sus servicios? (Ejemplos: nombre y apellido, DNI, N° de legajo, sexo, ocupación, carrera, etc.) Especificar.

Utilidad de los datos

5. ¿Con qué fines se registran los datos personales de los usuarios? (Puede seleccionar más de uno)

Selecciona todos los que correspondan.

Proporcionar servicios
Análisis estadísticos
Contacto
Mejorar la experiencia del usuario
Identificación
Otro:

Conservación y eliminación de datos

6. La base de datos en donde se almacena la información de los usuarios, ¿está incluida en el Registro Nacional de Bases de Datos Personales (RNBD)?

Sí
No

7. ¿En qué circunstancias la biblioteca decide eliminar los datos personales de un usuario? Especificar.

8. ¿La biblioteca almacena información respecto al historial de préstamos y devoluciones de los usuarios?

Sí
No

9. ¿Con qué frecuencia se elimina el historial de préstamo de los usuarios?

Nunca

Rara vez
A veces
Casi siempre
Siempre

10. En su biblioteca, ¿han ocurrido situaciones de riesgo que puedan haber resultado en la divulgación de datos personales de los usuarios? (Ejemplos: el acceso no autorizado a registros de usuarios, pérdida o robo de dispositivos que contengan datos sensibles de los usuarios, ciberataques, etc.)

Sí
No

USUARIOS

Derechos de los usuarios

11. ¿Se le notifica al usuario respecto de los derechos que tiene sobre la información proporcionada a la biblioteca, según la Ley 25.326 de Protección de los Datos Personales?

Sí
No

12. En caso de que su respuesta sea afirmativa, especificar qué información se les proporciona.

13. ¿Se les permite a los usuarios acceder, actualizar o suprimir los datos personales que constan en la biblioteca?

Sí
No

14. En caso de que haya existido o exista una situación de riesgo por la que se divulgue información de identificación personal de los usuarios, ¿se les notifica esta situación?

Sí
No

Consentimiento

15. ¿Se les solicita a los usuarios la firma de un consentimiento para el uso de sus datos personales?

Sí

No

SIGB Y SERVICIOS WEB

Sistemas Integrados de Gestión Bibliotecaria

16. A la hora de implementar el SIGB que utiliza la biblioteca, ¿se tuvieron en cuenta las políticas de privacidad ofrecidas por dicho software?

Sí

No

Correos Electrónicos

17. ¿Qué medidas de protección de datos personales implementa la biblioteca al momento de enviar correos electrónicos?

Ocultar remitentes cuando se trata de correos electrónicos masivos.
Correos electrónicos cifrados.
Software de seguridad de correo electrónico.
Eliminación periódica de correos electrónicos.
Opción de declinar servicios o cambiar dirección de correo electrónico.
No se aplica ningún tipo de medida.
Otro:

Redes Sociales

18. ¿Su biblioteca utiliza redes sociales para proveer o informar sobre servicios?

Sí

No

19. En caso de que la respuesta anterior haya sido afirmativa, ¿se implementa algún protocolo de uso de redes sociales que involucre la protección de los datos personales de los usuarios? Especificar.

Acuerdos con terceros

20. ¿La biblioteca tiene acuerdos con terceros, tales como colaboración con otras bibliotecas, préstamo interbibliotecario, proveedores de bases de datos, revistas académicas, empresas de tecnología, etc.?

Sí. Continua a la pregunta 20.1
No. Continua a la pregunta 21

20.1. ¿Se transfieren datos personales a terceros a la hora de efectuar una consulta que involucre a los usuarios?

Sí
No

20.2. Si la respuesta anterior fue afirmativa: ¿Los datos personales de los usuarios son anonimizados antes de ser transferidos a terceros?

Sí. Continua a la pregunta 21
No. Continua a la pregunta 21

FORMACIÓN DE USUARIOS Y DEL PERSONAL BIBLIOTECARIO

Capacitación de los usuarios sobre PDP

21. Desde la biblioteca, ¿se brindan capacitaciones destinadas a usuarios sobre la protección de datos personales?

Sí
No

Capacitación personal bibliotecario sobre PDP

22. ¿El personal bibliotecario ha recibido capacitación respecto a protección de datos personales?

Sí
No