UNIVERSIDAD MAYOR

# POLÍTICA DE PROTECCIÓN DE DATOS

# POLÍTICA DE PROTECCIÓN DE DATOS
# UNIVERSIDAD MAYOR

## I. Objeto

Atendido que gran parte de nuestras actividades en sociedad conllevan la entrega y recepción de distintos tipos de datos e información, el legislador ha demostrado una creciente preocupación en la regulación y protección de los datos personales y los procesos en los cuales se utilicen.

El propósito de esta política es establecer los principios, normas y lineamientos que garanticen la protección de los datos personales recopilados, almacenados y tratados por Universidad Mayor.

Esta política tiene como objetivo principal asegurar el cumplimiento de las normas, buenas prácticas y leyes aplicables respecto a la protección de datos personales. Así mismo, busca promover una cultura de respeto y responsabilidad ética en el tratamiento de los datos personales de toda nuestra comunidad universitaria, proveedores y personas externas cuando corresponda. Finalmente, mediante esta política se reconoce la importancia de implementar medidas de seguridad y protección de datos adecuadas que prevengan el acceso no autorizado; la divulgación, alteración o destrucción indebida de los datos personales bajo responsabilidad de la universidad.

## II. Alcance

Toda la comunidad universitaria deberá respetar y velar por el cumplimiento de la presente política. De forma especial, toda persona y/o terceros encargados del tratamiento de datos personales de cualquier índole y que mantengan una relación contractual y/o comercial con la Universidad Mayor serán debidamente informados y estarán obligados a cumplir con los principios y normas establecidos en la presente política.

## III. Marco Normativo

- Constitución Política de la República de Chile.
- Ley N° 19.628, sobre Protección de los Datos Personales.
- Ley N° 19.496, que Establece normas sobre protección de los derechos de los consumidores.

## IV. Declaración institucional

La Universidad Mayor reconoce la importancia de la persona humana y sus circunstancias inherentes tales como sus atributos, sus datos personales y la importancia de ellos en el cumplimiento de la misión institucional. Debido a lo anterior, la Universidad Mayor para los efectos de asegurar que el tratamiento de los datos personales bajo su responsabilidad se ejecute de forma legal, ética, justa y transparente, estará a lo dispuesto en la normativa nacional vigente, como asimismo en los estándares establecidos a nivel internacional que adopte.

La Universidad Mayor contempla los siguientes principios como base fundamental para la protección de los datos.

| Principio | Descripción |
|---|---|
| **Legalidad o licitud** | Los tratamientos de datos personales sólo pueden tratarse con sujeción a la ley. Se ha de determinar en cada tratamiento la fuente de legalidad correspondiente. |
| **Especificación de la finalidad** | Las finalidades de los tratamientos de datos personales deben ser específicos, deben estar relacionados con la actividad del responsable de tratamiento, y han de comunicarse claramente al titular de los datos antes de la recopilación o uso inicial, utilizando un lenguaje comprensible y adecuado. No se deben utilizar los datos para fines diferentes a aquellos para los cuales fueron |

| | |
|---|---|
| | recopilados originalmente, salvo en aquellos casos que la ley lo permita explícitamente. |
| **Elección y Consentimiento** | Los titulares de datos tienen el derecho de decidir cómo se utiliza su información personal. La universidad debe obtener el consentimiento explícito de los individuos para recopilar o procesar sus datos personales, informarles sobre sus derechos y proporcionarles la capacidad de retirar su consentimiento fácilmente. El consentimiento debe ser libre, específico, inequívoco e informado. |
| **Limitación de la Recopilación** | Las acciones de recopilación de datos personales deben limitarse a lo estrictamente necesario. La universidad debe evitar recopilar datos personales de manera indiscriminada, asegurándose de documentar y justificar la necesidad de los datos recolectados. |
| **Minimización de datos personales** | Se debe limitar la cantidad de datos personales disponibles, garantizando la adopción de un principio de "necesidad de saber". Es decir, se debe evaluar en cada caso la necesidad del uso de datos personales de acuerdo con los fines especificados. |
| **Limitación en el Uso** | La utilización de datos personales debe ser adecuado, relevante y no excesivo en relación con los fines para los que se recopilan. Se otorgará acceso al personal solo cuando sea necesario para el desempeño de sus funciones. |
| **Limitación de la Retención** | Se han de conservar los datos personales únicamente durante el tiempo necesario para cumplir con los fines para los que se recopilaron, luego deberá ser destruida o anonimizada de manera segura para su archivado, a menos que existan obligaciones legales, contractuales o normativas que requieran lo contrario. |
| **Limitación de la comunicación y transferencia** | La comunicación o divulgación y transferencia de datos personales deben realizarse de acuerdo con la ley aplicable y con el consentimiento del titular de los datos cuando sea necesario. Se deben establecer medidas adecuadas |

| | |
|---|---|
| | para garantizar la seguridad y protección de los datos personales durante la comunicación y transferencia.<br><br>La comunicación o transferencia de datos personales a otra entidad debe estar debidamente respaldada por un contrato o acuerdo entre las partes, cuando corresponda. Además, se debe evaluar especialmente la legalidad de la transferencia internacional de datos personales. |
| **Exactitud y Calidad** | Se debe garantizar que los datos personales sean precisos, actualizados y relevantes para los fines para los que se tratan. Además, se debe establecer mecanismos para corregir o actualizar la información si es necesario. |
| **Transparencia** | Se debe informar a los titulares de los datos sobre las prácticas de tratamiento de datos, incluyendo al menos los fines del tratamiento, la identidad del responsable del tratamiento y los derechos que les asisten como titulares de datos personales. Esto incluye notificar a los titulares sobre cualquier cambio importante en los procedimientos de manejo de datos personales. |
| **Responsabilidad** | El procesamiento de datos personales conlleva la responsabilidad de proteger la información y adoptar medidas concretas para ello. Estas medidas deben ser proporcionales al riesgo y promover la transparencia y honestidad. |
| **Seguridad** | Se deben implementar medidas técnicas y organizativas adecuadas para proteger los datos personales contra el acceso no autorizado; la divulgación, alteración o destrucción indebida. Estos controles se han de implementar de acuerdo con la probabilidad e impacto de los riesgos que conllevan. |
| **Confidencialidad** | El responsable y/o encargado de datos personales y quienes tengan acceso a ellos deberán guardar secreto o confidencialidad acerca de los mismos. El responsable establecerá controles y medidas adecuadas para preservar el secreto o confidencialidad. Este deber subsiste aún después de concluida la relación con el titular. |

| | |
|---|---|
| **Derechos del Titular** | Garantizar el ejercicio de los derechos de los titulares de datos personales, como el derecho de acceso, rectificación, cancelación o supresión, oposición, portabilidad y bloqueo (derechos ARCOP). |
| **Cumplimiento** | Cumplir con las leyes de protección de datos implica verificar y demostrar el cumplimiento de los requisitos de protección de datos mediante auditorías regulares, establecer controles internos adecuados y colaborar con las autoridades de supervisión. |

## V. Definiciones

| Concepto | Descripción |
|---|---|
| **Datos personales** | Cualquier información vinculada o referida a una persona natural identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante uno o más identificadores, tales como el nombre, el número de cédula de identidad o pasaporte, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. Para determinar si una persona es identificable, deben considerarse todos los medios y factores objetivos que razonablemente se podrían usar para dicha identificación en el momento del tratamiento. |
| **Datos personales sensibles** | Tendrán esta condición aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, que revelen el origen étnico o racial, la afiliación política, sindical o gremial, situación socioeconómica, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico y genético humano, los datos |

| | |
|---|---|
| | biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural. Adicionalmente, la Universidad considerará la información financiera y laboral de las personas como datos sensibles. |
| **Tratamiento de datos** | Cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan de cualquier forma recolectar, almacenar, acceder, procesar, comunicar, transferir, utilizar, actualizar, archivar o destruir datos personales. |
| **Titular de datos** | Se refiere a la persona natural a quien corresponden los datos personales que están siendo tratados. |
| **Responsable del tratamiento** | Persona jurídica que decide sobre los fines y medios del tratamiento de datos, es decir Universidad Mayor. |
| **Encargado del tratamiento** | Persona natural o jurídica que trata los datos por cuenta del responsable del tratamiento. |
| **Consentimiento** | Toda manifestación de voluntad libre, específica, inequívoca e informada, otorgada a través de una declaración o una clara acción afirmativa, mediante la cual el titular de datos, su representante legal o mandatario, según corresponda, autoriza el tratamiento de los datos personales que le conciernen. |
| **Derechos ARCOP** | Derechos de Acceso, Rectificación, Cancelación o Supresión, Oposición y Portabilidad que asisten al titular de datos personales para ejercer control sobre su información. |
| **Derecho de acceso** | Derecho del titular de datos a solicitar y obtener del responsable, confirmación acerca de si sus datos personales están siendo tratados, pudiendo acceder a ellos en los casos y condiciones que determine la ley. |
| **Derecho de rectificación** | Derecho del titular de datos a solicitar y obtener del responsable, que modifique o complete sus datos personales, cuando están siendo tratados |

| | |
|---|---|
| | por él, y sean inexactos, desactualizados o incompletos, en los casos y condiciones que determine la ley. |
| **Derecho de supresión** | Derecho del titular de datos a solicitar y obtener del responsable, que suprima o elimine sus datos personales, de acuerdo con las causales previstas en la ley. |
| **Derecho de oposición** | Derecho del titular de datos a solicitar y obtener del responsable, que no se lleve a cabo un tratamiento de datos determinado, de conformidad a las causales previstas en la ley. |
| **Derecho a la portabilidad** | Derecho del titular de datos a solicitar y obtener del responsable, una copia de sus datos personales en un formato electrónico estructurado, genérico y de uso común, que permita ser operado por distintos sistemas, y poder comunicarlos o transferirlos a otro responsable de datos. |
| **Comunicación** | Dar a conocer por el responsable de datos, de cualquier forma, datos personales a personas distintas del titular a quien conciernen los datos, sin llegar a cederlos o transferirlos. |
| **Transferencia** | Comunicación de datos personales a terceros ubicados en territorios o jurisdicciones distintas a las del responsable. |
| **Cesión** | Se refiere a la entrega o traspaso de datos personales a otra entidad o persona que se convierte en el nuevo responsable del tratamiento de esos datos. En este caso, la entidad que cede los datos concede la responsabilidad de estos al receptor, quien puede definir sus propios fines de tratamiento. |

## VI. Ámbitos de Acción

La Universidad Mayor desarrollará un **Sistema de Gestión de Privacidad de la Información (SGPI)** para asegurar una adecuada implementación de la presenta política, procurando gestionar

los riesgos de protección de datos mediante la aplicación de los controles necesarios para su mitigación, además de asegurar una adecuada actuación frente a posibles brechas de seguridad.

El SGPI se ocupará de los siguientes ámbitos de acción:

**a) Gobernanza de la protección de datos**

a. **Alineación con la estrategia institucional:** El SGPI asegurará que las obligaciones regulatorias, los requisitos contractuales y el alineamiento con los objetivos institucionales estén en línea con las mejores prácticas de la industria y los estándares aplicables en materia de protección de datos.
b. **Políticas, procedimientos y plan de concientización:** Definición de la estructura organizativa, roles y responsabilidades. Implementación de políticas de protección de datos claras y procedimientos operativos, complementados con programas de formación y concientización para todo el personal.
c. **Medición y evaluación:** Implementación de métricas, auditorías y revisiones periódicas para medir la efectividad del SGPI, así como la creación de informes anuales que permitan un monitoreo continuo del desempeño del sistema.

**b) Gestión de la Protección de datos**

a. **Evaluación de Impacto en Protección de Datos (EIPD):** Se aplicarán metodologías de evaluación de impacto en la protección de datos para identificar y mitigar riesgos en los procesos de tratamiento de datos de alto impacto en los derechos y libertades de las personas.

b. **Registros de Actividades de Tratamiento (RAT):** Mantener registros detallados y actualizados de todas las actividades de tratamiento de datos personales para asegurar la trazabilidad y el cumplimiento normativo.

**c) Operaciones de Protección de Datos**

a. **Aviso de protección de datos:** Asegurar que los titulares de los datos reciban información clara sobre cómo se recopilan y tratan sus datos personales, mediante un aviso de privacidad accesible y comprensible.
b. **Derecho a elección y Consentimiento:** Respetar las decisiones de los titulares sobre el uso de sus datos, garantizando la obtención de un consentimiento informado antes de realizar cualquier tratamiento.
c. **Privacidad por diseño y por defecto**: Se integrarán los principios de privacidad por diseño y por defecto en todos los proyectos, sistemas, aplicaciones y servicios de la universidad.
d. **Recolección limitada de Datos**: Implementar prácticas adecuadas para la recopilación de datos, asegurando que solo se recolecten los datos estrictamente necesarios para los fines especificados.
e. **Uso y Mantenimiento de Datos:** Asegurar que los datos sean usados de manera responsable y que se mantengan actualizados y precisos durante su ciclo de vida.
f. **Medidas de Seguridad:** Aplicar controles de seguridad técnicos y organizativos que aseguren la protección de los datos personales frente a accesos no autorizados, alteraciones o destrucción.
g. **Retención y Despersonalización**: Establecer políticas claras para la retención de datos, asegurando la anonimización o eliminación de estos una vez que ya no sean necesarios para los fines establecidos.

h. **Comunicación de Datos:** Regular la comunicación de datos dentro de la universidad y con terceros, asegurando que cualquier divulgación cumpla con las normas de privacidad aplicables.

i. **Transferencia de Datos:** Garantizar que las transferencias internacionales de datos cumplan con las normativas vigentes.

**d) Gestión de solicitudes ARCOP e Incidencias de Protección de Datos**

a. **Gestión de Solicitudes ARCOP**: Establecer procesos eficientes para manejar solicitudes de los titulares de los datos, asegurando que se respeten sus derechos de acceso, rectificación, cancelación o supresión, oposición y portabilidad

b. **Canal de comunicación:** Implementar mecanismos claros para gestionar las quejas y preocupaciones de los titulares de los datos respecto al tratamiento de su información.

c. **Gestión de Incidencias de Protección de Datos:** Desarrollar procedimientos para la detección, notificación y gestión de incidencias de seguridad que afecten la protección de datos, asegurando una respuesta rápida y mitigación del impacto.

d. **Cooperación con la Agencia de Protección de Datos:** Mantener una comunicación efectiva con las autoridades de protección de datos y cumplir con sus requerimientos de manera oportuna.

e. **Sanciones Administrativas Internas:** Se contemplarán mecanismos de sanción interna para los miembros de la comunidad universitaria que incumplan con las normativas de protección de datos, promoviendo una cultura de responsabilidad y respeto hacia la privacidad de los datos personales en todas las actividades y procesos.

## VII. Unidades a cargo

En la implementación del SGPI deberán colaborar activamente las direcciones de Gobierno de Datos y Analítica, de Ciberseguridad, de Control de Procesos y Gestión de Riesgos, y Auditoría Interna pertenecientes a la Contraloría, además de la Dirección de Tecnologías de la Información y la Secretaría General.

- **Dirección de Gobierno de Datos y Analítica:** responsable del desarrollo e implementación del SGPI.
- **Dirección de Ciberseguridad:** encargada de la seguridad de la información y la prevención de incidentes y brechas de datos personales.
- **Dirección de Control de Procesos y Gestión de Riesgos:** gestión de los riesgos relacionados con el tratamiento de datos personales.
- **Auditoría Interna:** verificación del cumplimiento de la política y el SGPI.
- **Dirección de Tecnologías de la Información**: implementación técnica de medidas de seguridad en la infraestructura tecnológica y de controles de privacidad por diseño y por defecto en sistemas y aplicativos.
- **Dirección de Cumplimiento**: Asesoría y verificación del cumplimiento normativo
- **Secretaría General:** Asesoría legal, y aplicación de sanciones administrativas.

### Delegado de Protección de Datos Personales (DPD)

El Delegado de Protección de Datos (DPD) deberá ser designado por la máxima autoridad de la universidad, quien o quienes se asegurarán de que el DPD cumpla con los requisitos de idoneidad, capacidad y conocimientos específicos para el ejercicio de sus funciones.

El DPD deberá contar con autonomía respecto de la administración en las materias relacionadas con el cumplimiento sobre la legislación aplicable en el ámbito de la protección de datos personales. El DPD podrá desempeñar otras funciones y cometidos, siempre y cuando no existan conflictos de interés con su labor.

Los titulares de datos podrán ponerse en contacto con el DPD en lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos ARCOP.

El DPD estará obligado a mantener estricto secreto o confidencialidad de los datos personales que conociere en ejercicio de su cargo.

Las autoridades de la universidad deberán disponer que el DPD cuente con los medios y facultades suficientes para el desempeño de sus funciones, debiendo otorgarle los recursos necesarios para realizar adecuadamente sus labores.

## VIII. Evaluación y actualización

La presente política podrá ser revisada en cualquier momento en el caso de ocurrencia de cambios legislativos o avances tecnológicos relevantes. Sin embargo, su evaluación no puede superar un periodo mayor a 24 meses desde la última revisión.

| Control de Cambios | | | | | | |
|---|---|---|---|---|---|---|
| N° Versión | Fecha Aprobación/Vigencia | Numeral (N° del título modificado) | Motivo del Cambio | Descripción del Cambio | Revisado por | Aprobado por |
| 1 | 17/12/2020 | No aplica | | Elaboración | Secretaría General | Rectoría |
| 2 | 01/05/2023 | No aplica | Creación y Separación materias | Política SGSI | Dirección De Ciberseguridad | Rectoría |
| 3 | 01/05/2023 | No Aplica | Separación materias | Política de Protección de Datos Personales | Dirección De Ciberseguridad | Rectoría |

UNIVERSIDAD MAYOR

PARA ESPÍRITUS EMPRENDEDORES