



UNIVERSIDAD MAYOR
para espíritus emprendedores

RCG/IDB/cbc

**APRUEBA POLÍTICA DE PROTECCIÓN
DE DATOS PERSONALES Y POLÍTICA
DE SEGURIDAD DE LA
INFORMACIÓN, QUE INDICA**

DECRETO N°15

Santiago, 17 diciembre de 2020

VISTOS:

- 1° La necesidad de establecer normativa interna, en materias de Ciberseguridad;
- 2° Las atribuciones que me confiere lo dispuesto en la letra m) del N° 3 del artículo 27 de los Estatutos de la Universidad Mayor.

CONSIDERANDO:

- 1° Que, de acuerdo al modelo educativo y al plan estratégico institucional, la Universidad Mayor reconoce la relevancia de actualizar y/o crear políticas e instructivos en el ámbito de la ciberseguridad;
- 2° Que, en atención a lo anterior, se hizo necesario crear un “proyecto de ciberseguridad” integrado por un grupo estable de miembros, compuesto por autoridades, directores, docentes y colaboradores de Universidad Mayor, para que establecieran el marco regulatorio, por medio de políticas específicas tendientes a proteger la información, como *activos tecnológicos*, y los datos personales, en este último caso, tanto de los miembros de la comunidad universitaria, como de los usuarios de las plataformas digitales asociadas a la Universidad;
- 3° Que, en razón del requerimiento descrito en el punto precedente, y como resultado del mismo, se elaboraron los siguientes instrumentos: “Política de Protección de Datos Personales” y “Política de Seguridad de la Información”, cuyo ámbito de aplicación, se extenderá a la toda la comunidad de Universidad Mayor, de ambas sedes, y;
- 4° Que, las Políticas antes referidas, se ajustan a la Reglamentación vigente de la Universidad Mayor.

DECRETO:

- 1° Apruébense, las “Políticas de Protección de Datos Personales” y “Política de Seguridad de la Información”;



UNIVERSIDAD MAYOR

para espíritus emprendedores

- 2° Adjúntense a continuación a la presente, una copia de las políticas aprobadas, y;
- 3° Cúmplase lo resuelto en el presente Decreto Universitario, a contar de esta misma fecha.

Regístrese, Comuníquese y Archívese.

Rubén Covarrubias Giordano, Rector–Inger Dahl Bravo, Secretaria General.

Lo que transcribo a Ud. para su conocimiento.

Le saluda atentamente,



INGER DAHL BRAVO

Secretaria General

Distribución:

- Vicerrectores
- Decanos
- Directores
- Archivo Secretaría General



UNIVERSIDAD MAYOR
para espíritus emprendedores

I. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

1. Información general

La presente Política de Protección de Datos Personales recoge el compromiso de la Universidad Mayor con el adecuado uso de los datos personales, el firme compromiso con el respeto de los derechos fundamentales y los valores propios de las sociedades democráticas. La Universidad Mayor es la responsable de todos los tratamientos de datos personales que se produzcan en y por la propia institución.

Mediante su Protección de Datos Personales, la Universidad Mayor informa a los usuarios del sitio web www.umayor.cl y todos los demás relacionados, así como a todos los miembros de la comunidad universitaria, que los datos personales a los que la Universidad tenga acceso serán tratados e incorporados a sus diferentes sistemas de gestión de información con pleno respecto a la normativa vigente en materia de protección de datos personales.

El **Oficial de Protección de Datos** de la Universidad Mayor es el encargado de informar, asesorar y supervisar la actividad de la Universidad respecto de los tratamientos de datos que se efectúen en la misma, además de formular recomendaciones al *Comité de Seguridad de la Información*. De igual modo, es el responsable de mantener actualizado el **“Documento de Seguridad en materia de Protección de Datos de la Universidad Mayor”**, texto de carácter reservado que contiene una descripción del conjunto de bases de datos de la Universidad y el nivel de riesgo asociado a cada una de ellas.

Además de lo anterior, actúa además como punto de contacto y de referencia para todos los miembros de la comunidad universitaria en las materias de su competencia.

2. Tratamientos de datos personales realizados.

Los diferentes tipos de tratamientos de datos personales efectuados por la Universidad Mayor en el ejercicio de sus obligaciones o funciones, tendrán la consideración de confidenciales y serán tratados por parte de ésta de acuerdo con la legislación vigente en materia de protección de datos personales.

Los datos personales que trata la Universidad Mayor proceden, normalmente, del propio titular de los mismos. En los casos en que no fuera así, en el primer contacto que la Universidad tenga con los titulares de dichos datos les informará del origen de sus datos y del tipo de tratamiento que se les da, salvo en los casos que las leyes le exceptúen de dicha obligación.



UNIVERSIDAD MAYOR

para espíritus emprendedores

Respecto de quienes siguen a la Universidad Mayor a través de sus cuentas en las redes sociales, el tratamiento de sus datos personales dejará de ser responsabilidad de la Universidad y se someterá a las políticas de protección de datos o de protección de la vida privada de la correspondiente red social de la que se trate.

Todos los tratamientos de datos personales efectuados en el ámbito de la Universidad Mayor se llevan a cabo adoptando las medidas de seguridad legalmente exigidas, tanto en sus instalaciones como en sus sistemas de información, atendiendo al riesgo que los diferentes tratamientos puedan suponer para los datos personales recabados. Asimismo, los miembros de la comunidad universitaria están obligados a respetar las citadas medidas de seguridad y a cumplir con ellas, asumiendo la responsabilidad por los daños y perjuicios que pudieran derivarse de su uso indebido. En el caso de los colaboradores, lo señalado precedentemente, será sin perjuicio de los deberes y obligaciones de fidelidad y secreto mencionados en los instrumentos contractuales respectivos, ya sea de índole laboral o de prestación de servicios.

Todos y cada uno de los tratamientos de datos efectuados por la Universidad tendrán alguna de las finalidades y bases legítimas descritas a continuación, de lo cual se informará a los titulares de los datos personales de forma expresa en los diferentes formularios o documentos en los que la Universidad recoja sus datos o, a más tardar, en la primera comunicación de la Universidad con los mismos.

3. Legitimidad de los tratamientos de datos personales realizados

La Universidad Mayor trata los datos personales de los miembros de la comunidad universitaria de forma legítima, con la finalidad de cumplir tanto con sus obligaciones legales como con su misión de vocación pública, sin perjuicio de las facultades que, como institución de educación superior, se le han atribuido. En el caso de que un tratamiento de datos personales requiera el consentimiento del titular de los datos, la Universidad lo exigirá dejando constancia de que el mismo se ha prestado de forma clara y expresa.

La base legal de cada una de las actividades de tratamiento llevadas a cabo por la Universidad Mayor es la Constitución Política de la República, en su artículo 19 N° 4, y la Ley N° 19.628.

4. Finalidades de los tratamientos y usos de los datos personales

Los datos personales que son responsabilidad de la Universidad Mayor serán tratados por la misma con las finalidades de gestión académica, docente e investigadora, para la tramitación y mantenimiento de la relación laboral correspondiente, para el control y la seguridad en las instalaciones universitarias, así como para la correcta gestión económica y



UNIVERSIDAD MAYOR

para espíritus emprendedores

financiera de la Universidad y de sus relaciones contractuales, además de la gestión de sus servicios de información, comunicación y difusión.

El **Oficial de Protección de Datos** llevará un registro de las actividades de tratamiento de datos personales indicando la base de legitimidad correspondiente.

Con la finalidad de prestar correctamente la misión que tiene encomendada como institución de educación superior, la Universidad Mayor podrá enviar información institucional sobre sus servicios y actividades a los miembros de la comunidad universitaria. Respecto de cualquier otra información que los interesados reciban, y para la que se hubieran suscrito, se podrán dar de baja en cualquier momento mediante el correspondiente procedimiento habilitado para ello.

Los datos personales recogidos de los diferentes miembros de la comunidad universitaria deberán ser datos verdaderos, exactos, completos y actuales. La Universidad Mayor, o, en su caso, la entidad que trabaje por cuenta de la misma implementará las medidas de seguridad necesarias para comprobar la identidad del usuario y resguardar sus datos, particularmente cuando se trate de datos sensibles y de menores de 18 años de edad.

El titular de los datos será el único responsable de cualquier daño o perjuicio, directo o indirecto, que pudiera ocasionar a cualquier persona a causa de la comunicación a la Universidad de datos falsos, inexactos, incompletos o no actualizados.

Asimismo, se informa que, las imágenes de los miembros de la comunidad universitaria, que aparezcan en cualquiera de los sitios web de la Universidad, o dependientes de la misma, han sido tratadas con total respeto a la normativa de protección de datos vigentes, así como también cuidando el respeto y protección a la vida privada y a la honra de la persona y su familia, así como el derecho a su propia imagen.

En consecuencia, la Universidad Mayor no autoriza a reproducir, distribuir y comunicar las imágenes fotográficas y videos que se encuentren en un sitio web de la Universidad, que no esté referido expresamente al contexto de la publicación original. La Universidad Mayor está exenta de cualquier responsabilidad por el incumplimiento de este requisito.

Más allá de estos usos, los datos personales tratados por la Universidad Mayor no serán comunicados a terceros ajenos a nuestra institución, salvo en los casos establecidos legalmente o cuando se cuente con la autorización inequívoca del titular de los mismos.

5. Datos especialmente protegidos

Conforme a la ley, son datos especialmente protegidos, aquellos datos personales que se refieren a, las características físicas o morales de las personas o a hechos o circunstancias



UNIVERSIDAD MAYOR

para espíritus emprendedores

de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

Como regla general, para el tratamiento de estos datos se requerirá el consentimiento inequívoco de su titular, sin perjuicio de que la Universidad Mayor tomará especiales medidas técnicas y organizativas para su protección, estando siempre en posición de demostrar que el señalado consentimiento ha sido prestado.

6. Conservación de los datos personales

Los datos personales tratados por la Universidad Mayor serán conservados por ésta mientras se mantenga la prestación del servicio o la relación laboral o contractual, durante el tiempo necesario para cumplir con la finalidad para la que fueron recogidos, o durante el tiempo previsto en la normativa correspondiente, así como para atender a las posibles responsabilidades derivadas de los tratamientos previamente efectuados.

7. Derechos de los titulares de los datos

Cualquier persona podrá ejercer los derechos de acceso, rectificación, cancelación (supresión), oposición y a no ser objeto de decisiones individuales automatizadas respecto de los datos que le conciernan y que sean tratados bajo la responsabilidad de la Universidad Mayor.

Dichos derechos, serán ejercitados frente al **Oficial de Protección de Datos** de la Universidad Mayor, a través de los medios digitales que se establezcan, adjuntando copia de la cédula de identidad del titular de los datos u otros documentos o modalidades que den certeza acerca de la identidad del solicitante. En el caso de actuaciones por representación, deberá probarse mediante las formas legalmente admitidas.

El **Oficial de Protección de Datos** contará con un máximo de 2 días hábiles para pronunciarse sobre las solicitudes que se le formulen.

8. Duración y modificación de la Política de Protección de Datos Personales

La Universidad Mayor, se reserva el derecho a modificar unilateralmente los términos y condiciones aquí estipulados, de forma total o parcial, con el objeto de adaptar su Política a las novedades legislativas, criterios jurisprudenciales, prácticas del sector o intereses de la institución. Cualquier cambio se pondrá en conocimiento de los miembros de la comunidad universitaria, con la debida antelación, a través del presente sitio web, así como por los medios que la Universidad estime convenientes.



UNIVERSIDAD MAYOR
para espíritus emprendedores

II. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

La Universidad Mayor considera que sus activos tecnológicos constituyen recursos estratégicos indispensables para alcanzar los objetivos de excelencia como institución de educación superior, entendiendo para estos efectos como **activos tecnológicos** el conjunto de los sistemas, redes y datos que están a disposición de la comunidad universitaria.

La Universidad Mayor ha definido como indispensable adoptar las medidas organizativas y técnicas necesarias para garantizar el pleno funcionamiento de los activos tecnológicos a fin de protegerlos frente a cualquier daño, sea accidental o provocado, que puedan afectar a la disponibilidad de los activos, la integridad de la información, su confidencialidad y la correcta autenticación de los usuarios, de forma de estar protegidos contra amenazas de rápida evolución que puedan vulnerar el valor y/o la calidad de la información y la continua prestación de servicios por parte de la Universidad.

En consecuencia, la consolidación del uso de las tecnologías de la información y las comunicaciones por la Universidad Mayor exige el establecimiento de un conjunto de medidas y procedimientos, para el tratamiento y gestión de los riesgos asociados a la seguridad de la información, de forma de constituir un **Sistema de Gestión de la Seguridad de la Información (SGSI)**, sistema complejo que implica la orientación a tal fin de personas, tecnologías, normas y procedimientos.

A manera ilustrativa, es del caso señalar que, por ejemplo, los cambios en la cultura organizacional en materia de seguridad de la información requerirán del apoyo de la Vicerrectoría de Desarrollo y Gestión; el control del cumplimiento de las actividades asociadas a la gestión de los riesgos requerirá de la intervención de la Contraloría y muchas de las decisiones requerirán del análisis de la Secretaría General de la Universidad.

Dentro de ese contexto, el propósito de la presente **Política de Seguridad de la Información** de la Universidad Mayor, en adelante, la Política, es establecer las bases de funcionamiento y operación de sus activos tecnológicos de forma de asegurar su efectiva prestación de servicios y el cuidado de la información, de forma de evitar interrupciones en su flujo de funcionamiento, modificaciones indebidas y fugas de información o conocimiento hacia personas y entidades no autorizadas.

La Universidad Mayor ha decidido que la seguridad de las tecnologías de la información y la comunicación es una parte integral de cada etapa del ciclo de vida de los activos tecnológicos, desde su etapa de implementación hasta su retirada de servicio, así como también en lo referido a decisiones de adquisición de equipamiento, desarrollo y explotación, adoptando **medidas de prevención** para reducir la posibilidad de que los riesgos lleguen a materializarse, contemplando normas y procedimientos que contemplen la disuasión y, en caso de materialización de los riesgos, la reducción del impacto de los mismos, así como la resiliencia de los sistemas críticos de información.



UNIVERSIDAD MAYOR

para espíritus emprendedores

Para lo anterior, y con el fin de garantizar la disponibilidad de los servicios críticos, la Universidad Mayor desarrollará: a) **planes de contingencia**; b) **planes de continuidad de negocio**; y c) **planes de recuperación ante desastres**, y, en ese contexto, definirá los roles y funciones de los miembros de la comunidad universitaria.

2. ÁMBITO DE APLICACIÓN

Esta Política de Seguridad de la Información, se aplica a la amplia generalidad de los activos tecnológicos gestionados y administrados por la **Dirección de Tecnologías de la Información** de la Universidad Mayor.

Quedan fuera del ámbito de aplicación de la presente Política, por no considerarse activos tecnológicos de la Universidad Mayor, aquellos computadores, procesadores de información o dispositivos personales financiados a título individual, no inventariados a nombre la Universidad, aunque ocasionalmente sean utilizados para labores propias de investigación, docencia o extensión.

No obstante, en el caso de que se acceda a las redes de comunicaciones electrónicas de la Universidad mediante tales elementos, quedarán sujetos a las obligaciones establecidas en la presente **Política de Seguridad de la Información**, sin perjuicio de que la Universidad, por decisión fundada del *Comité de Seguridad de la Información*, les pueda negar el acceso a sus redes si no cumplen con los requisitos de seguridad o plantean la razonable posibilidad de generar un eventual incidente que pueda comprometer la seguridad de la información de los activos tecnológicos o el buen nombre o imagen de la Universidad Mayor.

3. ORGANIZACIÓN DE LA SEGURIDAD

3.1. *Comité de Seguridad de la Información*

El Comité de Seguridad de la Información, en adelante, el Comité, tiene por rol velar por la efectiva vigencia de la **Política de Seguridad de la Información en la Universidad Mayor**, así como de los instructivos y documentos que se deriven de la presente Política. Está compuesta por las siguientes personas:

- 1) Contralor (quien lo preside).
- 2) Secretario General, o quien le represente.
- 3) Vicerrector de Desarrollo y Gestión, o quien le represente.
- 4) Oficial de Seguridad de la Información (CISO).
- 5) Oficial de Protección de Datos.
- 6) Director de Personas, o quien le represente.
- 7) Director de Comunicaciones Estratégicas, o quien le represente.
- 8) Director de Ciberseguridad, o quien le represente.
- 9) Director de Tecnologías de la Información, o quien le represente.

El Comité se reunirá a instancias del Contralor con una periodicidad mensual, salvo que la adopción de medidas urgentes aconseje otra medida distinta, y podrá invitar a sus



UNIVERSIDAD MAYOR

para espíritus emprendedores

reuniones a las personas que considere oportunas en función de los temas a tratar; el quorum para sesionar será el de la mayoría de sus miembros estables.

En materia de seguridad, el Comité tendrá las siguientes funciones:

- 1) Informar regularmente del estado de la seguridad de la información al Rector de la Universidad.
- 2) Promover la mejora continua del **Sistema de Gestión de la Seguridad de la Información (SGSI)**.
- 3) Elaborar la estrategia de evolución de la Universidad Mayor en lo que respecta a la seguridad de la información.
- 4) Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, evitando duplicidades.
- 5) Revisar regularmente la **Política de Seguridad de la Información** y realizar propuestas de mejora, y someterlas al Directorio de la Universidad para su aprobación.
- 6) Elaborar circulares o instrucciones en desarrollo de lo dispuesto en la **Política de Seguridad de la Información de la Universidad Mayor**.
- 7) Recomendar requisitos de formación y calificación de administradores, operadores y usuarios de los activos tecnológicos de la Universidad, desde el punto de vista de la seguridad de la información.
- 8) Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de dicha gestión.
- 9) Velar por la coordinación de las diferentes áreas de la Universidad en la gestión de incidentes de seguridad de la información.
- 10) Aprobar planes de mejora de la seguridad de la información de la Universidad Mayor.
- 11) Priorizar las actuaciones en materia de seguridad de la información cuando los recursos sean limitados.
- 12) Velar para que la seguridad de la información sea considerada en todos los proyectos de la Universidad, desde su planteamiento inicial hasta su puesta en operación.
- 13) Resolver los conflictos de responsabilidad que puedan aparecer entre los responsables de diferentes áreas, elevando al órgano competente aquellos casos en los que no tenga suficiente autoridad para decidir.
- 14) Velar por el efectivo respeto del derecho a la protección de datos personales en las operaciones de tratamiento de datos que lleve adelante la Universidad Mayor.

3.2. Oficial de Seguridad de la Información

El **Oficial de Seguridad de la Información** (llamado usualmente en inglés como CISO, por *chief information security officer*) es el responsable máximo en planificar, desarrollar, controlar y gestionar las políticas, procedimientos y planes de acción con el fin de implementar una efectiva seguridad de la información en la Universidad Mayor, teniendo especialmente a su cargo las decisiones sobre el cumplimiento regulatorio por parte de la



UNIVERSIDAD MAYOR

para espíritus emprendedores

misma, la continuidad del negocio en lo que a activos tecnológicos se refiere, y es el responsable último por las decisiones de seguridad corporativa.

De igual forma, son roles del Oficial de Seguridad de la Información:

- a) Establecer las acciones, mecanismos y protocolos para responder eficazmente a los incidentes de seguridad, así como implementarlos efectivamente.
- b) Constituirse en el punto de contacto para las comunicaciones con respecto a incidentes detectados en otras unidades y/o divisiones de la Universidad Mayor.

Para el desarrollo de sus labores cuenta con la debida colaboración de la **Dirección de Tecnologías de la Información** y de la **Dirección de Ciberseguridad**.

3.3. Dirección de Ciberseguridad

La Dirección de Ciberseguridad es una unidad académica centrada en la investigación, labor que realiza a través del **Centro de Investigación en Ciberseguridad**, con obligaciones específicas de colaboración a requerimiento del **Oficial de Seguridad de la Información**.

En este rol, la Dirección de Ciberseguridad tiene a su cargo el **Centro de Operaciones de Seguridad**, unidad responsable de **detectar e identificar** riesgos y amenazas, actuales y potenciales, que puedan poner en riesgo o dañar los activos tecnológicos de la Universidad Mayor, así como implementar medidas de **reacción**, a requerimiento del **Oficial de Seguridad de la Información** y en coordinación con la **Dirección de Tecnologías de la Información**.

A la Dirección de Ciberseguridad le corresponde, a requerimiento del *Comité de Seguridad de la Información*, establecer los protocolos para la colaboración y el intercambio de información relacionadas con incidentes con los **Equipos de Respuesta frente a Incidencias de Seguridad Informática (CSIRT)** públicos y/o privados del país o el extranjero, sin perjuicio de la facultad de la Universidad Mayor, de establecer en la **Dirección de Ciberseguridad**, un CSIRT propio de la Universidad Mayor que, en cualquier caso, será una herramienta de apoyo a la investigación y docencia.

Además, tiene deberes de coordinación respecto del **Centro de Operación de Redes**, dependiente de la **Dirección de Tecnologías de la Información**, a fin de que esta última pueda adoptar oportunamente las medidas técnicas y organizativas que le permitan **proteger** los activos de la Universidad ante un eventual ataque o falla, así como también la **recuperación** de dichos activos, en el caso de que el incidente dañoso ya se hubiere producido.

4. TERCERAS PARTES

Cuando la Universidad Mayor preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta **Política de Seguridad de la Información** y se establecerán canales para reporte y coordinación, además de establecer procedimientos de actuación para la reacción ante incidentes de seguridad.



UNIVERSIDAD MAYOR

para espíritus emprendedores

Ningún proyecto o colaboración que comprenda la interacción con tecnologías de la información y comunicación se llevará adelante sin tener identificado al **Oficial de Seguridad de la Información** de la otra institución, organismo o entidad, aun cuando formalmente no tenga dicho nombre, siendo lo relevante que dicha persona tenga la facultad de resolver los incidentes que se presenten.

Cuando la Universidad Mayor utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta **Política de Seguridad de la Información** y de la normativa de seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte, se requerirá un informe del Director de Ciberseguridad para que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por el Comité de Seguridad de la Información antes de seguir adelante.

5. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

La Universidad Mayor ha adoptado los más altos estándares que permiten garantizar el nivel de seguridad requerido por la normativa internacional en relación con la protección del tratamiento de los datos de carácter personal tanto de los miembros de la comunidad universitaria como de todos quienes, directa o indirectamente, participen de los estudios e investigaciones.

Para tales efectos, la “**Política de Protección de Datos Personales de la Universidad Mayor**” contiene los principios a los que se sujeta a Universidad en dicha materia, así como también la manera en que los miembros de la comunidad universitaria pueden ejercer sus derechos.

La señalada política se complementa con el “**Documento de Seguridad en materia de Protección de Datos de la Universidad Mayor**”, accesible exclusivamente para las personas autorizadas, como son los responsables de seguridad en materia de protección de datos de las bases de datos que contienen datos personales que hayan sido catalogadas de niveles de seguridad **medio** y **alto**, así como a quienes autorice el *Comité de Seguridad de la Información*.

Dicho documento recoge las bases de datos existentes en la Universidad Mayor, su nivel de importancia en cuanto a la naturaleza y finalidad de los datos que contiene, los responsables de cada uno de ellos y las medidas, normas, procedimientos y estándares encaminados a garantizar los niveles de seguridad exigidos, así como las funciones y obligaciones del personal a cuyo cargo se encuentren.

Todos los activos tecnológicos de la Universidad Mayor se ajustarán a los niveles de seguridad requeridos por la normativa interna en función de la naturaleza y finalidad de los datos de carácter personal cuya existencia es recogida en el “**Documento de Seguridad en materia de Protección de Datos de la Universidad Mayor**”.



UNIVERSIDAD MAYOR

para espíritus emprendedores

Es rol del **Oficial de Protección de Datos** de la Universidad Mayor mantener permanentemente actualizado el Documento de Seguridad, velar por el respeto de los principios de la protección de datos personales en el tratamiento que se haga de ellos desde su recogida hasta su destrucción, hacer efectivos los derechos de las personas en la materia y formular recomendaciones al *Comité de Seguridad de la Información* en las materias que son propias de sus competencias; además, debe comunicar al **Oficial de Seguridad de la Información** cualquier incidente o circunstancia que pueda comprometer la seguridad de los datos personales.

El **Oficial de Protección de Datos** puede ser el mismo **Oficial de Seguridad de la Información** u otra persona que se designe por el Rector mediante resolución, pero dichos roles nunca pueden recaer en el **Director de Tecnologías de la Información**, ni ser subordinados o estar en posición de dependencia respecto de este.

Sin embargo, no podrán estar ambos cargos en posesión de la misma persona si, a criterio del *Comité de Seguridad de la Información*, surgen conflictos de interés entre ambos roles o si ello afecta la autonomía del **Oficial de Protección de Datos** para formular recomendaciones al *Comité*.

Todo usuario interno o externo que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con la Universidad Mayor.