Universidad Mayor | Dirección de Tecnologías de la Información

POLÍTICA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES

POLÍTICA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES[1]

I. OBJETO

El objetivo de esta Política es establecer los lineamientos y requisitos que deben cumplir los proveedores externos, subcontratistas y terceros que prestan servicios a La Universidad Mayor en materia de seguridad de la información. Con el fin de garantizar la calidad de los servicios y el cumpliendo de las obligaciones contractuales.

Mantener un nivel adecuado de seguridad de la información de los servicios contratados, a través de la implementación de acuerdos, la supervisión de su cumplimiento y la gestión de cambios para garantizar que los servicios se entreguen de manera segura.

II. ALCANCE

Esta política comprende toda relación comercial existente entre la Universidad Mayor y sus proveedores y empresas contratistas, ya sea a través de un contrato u otro tipo de acuerdo por escrito, incluyendo relaciones derivadas únicamente de la emisión y aceptación de una orden de compra. Aborda temáticas de seguridad, que apliquen a proveedores y/o contratistas que presten servicios a La Universidad Mayor incluyendo:

- Servicios de tratamiento o resguardo de información, tales como hosting, infraestructura, plataforma tecnológica, centros de datos y procesamiento, almacenaje de información física o digital, entre otros.
- Sistemas de información desarrollados para La Universidad Mayor.

[1] Política aprobada mediante Decreto Nro. 37 de fecha 01 de agosto de 2025.

Documento Controlado, prohibida su reproducción parcial o total sin autorización

- Hardware, software o cualquier otro tipo de equipo tecnológico.
- Servicios de consultoría, capacitación o asistencia técnica.

Se deberán respetar, además, los acuerdos específicos adquiridos en cada uno de los contratos particulares que detallan las modalidades especiales y condiciones comerciales que se aplican respecto del proveedor y/o contratista del caso.

III. DECLARACIÓN INSTITUCIONAL

La Universidad Mayor reconoce que la adecuada gestión de proveedores, contratistas y terceros constituye un elemento estratégico para garantizar la seguridad de la información, la continuidad operativa y el cumplimiento normativo de la institución. Dado que los servicios externos pueden involucrar el acceso, tratamiento y resguardo de información crítica, la Universidad declara su compromiso de establecer lineamientos claros y exigentes que aseguren la calidad, la seguridad y la confidencialidad en cada relación contractual.

IV. MARCO NORMATIVO

Para la elaboración de esta Política se ha tenido a la vista y se ha considerado la siguiente normativa:

- Ley N° 19.628 sobre Protección de Datos Personales.
- Ley N° 21.663 sobre Ciberseguridad e Infraestructura Crítica de la Información.
- Ley N° 21.459 sobre Normas sobre delitos informáticos.
- Política Protección de Datos.
- Política de Gestión de Seguridad de la Información.
- Política de Gestión de Incidentes de Seguridad de la Información.

Documento Controlado, prohibida su reproducción parcial o total sin autorización

V. DEFINICIONES

Para efectos de la presente Política se entenderá por:

Concepto	Descripción
Acuerdo de Nivel de Servicio (ANS o SLA):	Documento formal que establece los compromisos, métricas, tiempos de respuesta y niveles de calidad exigidos al proveedor respecto a los servicios contratados.
Confidencialidad	Obligación de proteger la información de la Universidad Mayor contra accesos, usos o divulgaciones no autorizadas, garantizando su resguardo conforme a los marcos legales y normativos.
Disponibilidad	Garantía de que los servicios e información contratados estarán accesibles y utilizables en el momento requerido, de acuerdo con las necesidades de la Universidad Mayor.
Integridad	Propiedad que asegura que la información mantenida o procesada por proveedores no sea alterada de manera indebida o no autorizada.
Incidente de Seguridad de la Información	Evento inesperado que afecta o puede afectar la confidencialidad, integridad o disponibilidad de la información y servicios de la Universidad Mayor, originado en las operaciones de un proveedor.

VI. ÁMBITOS DE ACCIÓN

1. Requisitos de seguridad

En cada solicitud de contratación de servicios, se deben especificar los requisitos mínimos de seguridad para cualquier proveedor que necesite acceder a recursos, información o instalaciones de La Universidad Mayor para llevar a cabo su servicio. En estos casos, los proveedores deben cumplir con los siguientes requisitos de seguridad:

- Contar con mecanismos y controles de seguridad adecuados para proteger la información y los activos de la Universidad Mayor.
- Realizar una evaluación de riesgos de seguridad asociados al servicio entregado.

Documento Controlado, prohibida su reproducción parcial o total sin autorización

- Permitir a la Universidad Mayor realizar auditorías de seguridad a sus instalaciones y sistemas.
- Suscribir un acuerdo de confidencialidad y no divulgación de información.
- Implementar medidas de seguridad para el intercambio de información de la Universidad Mayor.
- Establecer y documentar procedimientos para la gestión de incidentes de seguridad.
- Mantener la disponibilidad permanente de los servicios entregados.
- Permitir a la Universidad Mayor realizar un monitoreo de los servicios tecnológicos externalizados.

Los proveedores solo pueden realizar las actividades descritas en el contrato. Deben informar a la Universidad Mayor sobre su personal, perfiles y responsabilidades, y notificar cualquier cambio en esta información.

Todo proveedor de servicios que tenga acceso (con o sin privilegios) a los sistemas de información la Universidad Mayor, independientemente de su ubicación o la infraestructura utilizada, deberán cumplir con las Políticas de Seguridad de la organización. Esto incluye los controles y cuidados relacionados con el acceso a la información descritos en la Política de Control de Acceso.

El Director de Tecnología de la Información es la persona responsable de analizar y aprobar el acceso a los sistemas de la Universidad Mayor a aquellas personas o entidades que tengan un vínculo contractual con la empresa, así como los trabajadores y contratistas que requieran dicho acceso para el desarrollo de sus funciones.

A su vez, el personal técnico de la Dirección de Tecnologías de la Información de la Información es responsable de controlar el acceso a los servicios de red y los sistemas de procesamiento de datos con el fin de evitar que los usuarios comprometan la seguridad de la red y sus servicios.

Restricciones de uso de la red

Con el objetivo de garantizar la seguridad y el buen funcionamiento de la red, se establecen las siguientes normas para el uso de internet por parte de los proveedores de servicio:

Documento Controlado, prohibida su reproducción parcial o total sin autorización

- Los proveedores podrán acceder únicamente al segmento de internet designado para ellos, quedando prohibida su conexión a la red principal o a cualquier otro segmento no autorizado.
- El acceso a la red solo estará permitido a través de dispositivos previamente autorizados por la Dirección de Tecnologías de la Información. La conexión de equipos no autorizados resultará en la expulsión inmediata del personal de la faena involucrada, con prohibición de ingreso hasta que la empresa contratista resuelva el incidente y garantice mediante acciones concretas la toma de medias para que lo sucedido no vuelva a ocurrir.
- El uso no autorizado de la red será tratado como una violación a la seguridad de la información, por tanto, se responsabilizará a la empresa proveedora por las acciones de su personal y deberá asumir las consecuencias legales que se deriven de cualquier infracción a las normas establecidas.
- En caso de tráfico sospechoso o actividad maliciosa, la universidad Mayor podrá solicitar la retirada del equipo hasta que la empresa proveedora presente un documento de compromiso para la revisión y limpieza de este.

La Universidad Mayor, se reserva el derecho de monitorear la actividad de los proveedores en la red. El personal técnico de la Dirección de Tecnologías de la Información, en caso de detectar equipos involucrados en actividades maliciosas, como el uso de software pirata, descarga de archivos ilegales, ataques a la red o cualquier otra actividad maliciosa, procederá al bloqueo inmediato de los accesos y la desconexión del equipo involucrado. Se debe notificar al director de tecnología de la información el evento o incidente para que se registre en el sistema dispuesto por la Universidad Mayor según lo descrito en la política de Gestión de Incidentes de Seguridad de la Información.

1.1. Cláusulas contractuales de seguridad

Con el fin de establecer contratos y acuerdos rigurosos en materia de seguridad, se debe detallar los requisitos más relevantes en los contratos con los proveedores. Todos los aspectos se deben estipular en acuerdos de confidencialidad y de accesos a datos, como:

- Determinar a qué información acceden, cómo acceden y la clasificación y protección de esta.

Documento Controlado, prohibida su reproducción parcial o total sin autorización

- Garantizar que, una vez finalizado el contrato, el proveedor ya no pueda acceder o mantener la información sensible de la Universidad Mayor
- Reflejar los requisitos legales, como cumplimiento de los derechos de propiedad intelectual, cumplimiento de protección de datos, entre otros.
- Estipular el derecho de auditorías y de controles sobre la seguridad de los sistemas o servicios contratados.
- Incluir las situaciones que conlleven a la finalización del contrato.
- Definir las garantías específicas, como penalizaciones económicas en caso de incumplimiento, perjuicios económicos por inactividad y garantías adicionales.
- Compromiso que obligue a cumplir todas las políticas de seguridad de la universidad Mayor, esto incluye, entre otros requisitos:
    - Mantener actualizado el software antivirus y antimalware en todos sus equipos.
    - Capacitar a su personal en materia de seguridad informática.
    - Notificar a la dirección de tecnología de la información de forma inmediata cualquier evento o incidente de seguridad que pueda afectar a la red.

1.2. Definición de Acuerdos de Nivel de Servicio

Los Acuerdos de Nivel de Servicio (ANS o SLA en inglés) establecen las características de calidad y las garantías del servicio adquirido, siendo necesario definir y firmar los ANS correspondiente con los proveedores. Los aspectos más relevantes para definirlos son:

- Responsabilidades de cada una de las partes.
- Duración del acuerdo.
- Detalle del nivel de servicio ofrecido. Incluyendo:
    - Tasas de error permitidas.
    - Disponibilidad horaria.
    - Tiempos de respuesta y resolución.

Documento Controlado, prohibida su reproducción parcial o total sin autorización

- Canales de contacto.
- Proceso de escalado y notificación ante incidentes.
- Procedimientos para la resolución de problemas e incidencias.
- Personal asignado al servicio.

- Medición de la satisfacción por el servicio recibido.

1.3. Confidencialidad y Protección de los Datos

El contrato debe establecer medidas para proteger la confidencialidad de la información compartida entre La Universidad Mayor y el proveedor. Esto es especialmente relevante en casos donde se comparten datos sensibles o estratégicos.

Las medidas de protección de datos pueden incluir:

- Acuerdo de confidencialidad que obligue al proveedor a mantener la confidencialidad de la información compartida.
- Cláusulas contractuales específicas que establezcan cómo se debe tratar la información confidencial, incluyendo:
  - Restricciones en el uso y la divulgación de la información.
  - Obligaciones de seguridad para proteger la información contra el acceso no autorizado, la pérdida, el robo o la destrucción.
  - Mecanismos para la resolución de disputas relacionadas con la confidencialidad.
  - Medidas técnicas de seguridad para proteger la información, como el cifrado, el control de acceso y la monitorización de la seguridad.

1.4. Finalización de la relación contractual

Es importante garantizar la seguridad de la información tras la finalización de los servicios contratados. Para ello se debe formalizar las acciones a realizar una vez finalizado el servicio:

Documento Controlado, prohibida su reproducción parcial o total sin autorización

- Señalar los activos que han de ser devueltos.
- Eliminación de permisos de acceso.
- Borrado de información sensible de la Universidad Mayor almacenada en los sistemas del proveedor.
- El proveedor deberá entregar a la Universidad Mayor un documento que acredite la eliminación segura de la información.

1.5. Difusión

La Universidad Mayor implementará actividades para difundir esta y todas las políticas de seguridad de la información con el objetivo de concientizar al personal interno y externo que presten servicio para la organización. Estas actividades incluirán la publicación en medios que la Universidad Mayor disponga, como secciones dedicadas a la Seguridad de la Información en los sitios web internos, la difusión a través de correo electrónico, y la integración en los procesos de inducción del personal nuevo y en los contratos con terceros. Además, de ser compartida a los proveedores.

1.6. Evaluación y Seguimiento

Durante la duración del contrato, se acordarán procesos para evaluar y hacer seguimiento al desempeño del proveedor. Esto asegura que se cumplan los objetivos establecidos y permite realizar ajustes si es necesario.

1.7. Aceptación de las normas

La firma de un acuerdo contractual por parte de los proveedores de servicio implica la aceptación de las normas y condiciones descritas en este documento.

VII. UNIDAD(ES) A CARGO

La implementación, seguimiento y actualización de la presente Política estará a cargo de la Dirección de

Documento Controlado, prohibida su reproducción parcial o total sin autorización

Tecnologías de la Información.

VIII. EVALUACIÓN Y ACTUALIZACIÓN

La evaluación de la presente Política será de carácter anual, pudiendo actualizarse cuando sea necesario o cuando un cambio normativo o legal así lo amerite.

Documento Controlado, prohibida su reproducción parcial o total sin autorización

Control de Cambios						
N° Versión	Fecha Aprobación/Vigencia	Numeral (N° del título modificado)	Motivo del Cambio	Descripción del Cambio	Revisado por	Aprobado por
1	01/08/2025		Versión original	Versión original	Jefe Calidad y Servicios	Director de Tecnologías de Información

UMAYOR.CL - 600 3281000

5 AÑOS

ACREDITADA

• Gestión Institucional
• Docencia de Pregrado
• Vinculación con el Medio

Desde 20 mayo 2015
Hasta 20 mayo 2020

Comisión Nacional de Acreditación
CNA-Chile