Universidad Mayor | Dirección de Tecnologías de la Información

POLÍTICA DE GESTIÓN DE ADMINISTRACIÓN DE ACTIVOS DE INFORMACIÓN

POLÍTICA DE ADMINISTRACIÓN DE ACTIVOS DE INFORMACIÓN[1]

I. OBJETO

El objetivo de esta Política es definir las obligaciones y derechos de los trabajadores de la Universidad Mayor en lo que respecta al empleo de recursos informáticos, tecnológicos y activos de información en general.

II. ALCANCE

Esta política establece los lineamientos y responsabilidades para la gestión segura de los activos de información, equipos y plataformas de servicios informáticos pertenecientes a la Universidad Mayor o de sus clientes. El alcance incluye:

- Activos de información: Toda la información generada, recibida, procesada, transmitida o almacenada por la organización, independientemente de su formato o soporte (físico o digital).
- Equipos: Computadores personales, laptops, servidores, dispositivos móviles, redes, etc.
- Plataformas de servicios informáticos: Sistemas operativos, software de aplicación, bases de datos, correo electrónico, internet, etc.
- Usuarios: Todos los individuos que acceden o utilizan los activos de información, equipos y plataformas de servicios informáticos de la Universidad Mayor, incluyendo empleados, alumnos y proveedores.

III. DECLARACIÓN INSTITUCIONAL

La Universidad Mayor reconoce la importancia estratégica de los activos de información, los equipos tecnológicos y las plataformas de servicios informáticos como recursos esenciales para el desarrollo de sus funciones académicas, administrativas y de gestión. En este contexto, declara su compromiso de garantizar una administración responsable, segura y eficiente de dichos activos, asegurando que su uso contribuya al cumplimiento de los objetivos institucionales.

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

Con esta política, la Universidad se compromete a proteger la confidencialidad, integridad y disponibilidad de sus activos de información y recursos tecnológicos, promoviendo un uso ético, transparente y conforme a la legislación vigente. Asimismo, establece lineamientos claros que permiten prevenir riesgos, reducir vulnerabilidades, asegurar la continuidad de los procesos críticos y fomentar una cultura institucional de resguardo y responsabilidad compartida en la gestión de la información y la tecnología.

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.
- Decreto 16 de 2020: Seguridad para uso de correos electrónicos institucionales y uso de servicio de internet.
- Política de uso de correo institucional.

V. DEFINICIONES

Para efectos de la presente Política se entenderá por:

Concepto	Descripción
Activos:	Se refiere a los elementos valiosos, ya sean tangibles o intangibles, que posee una organización y que contribuyen a su funcionamiento y éxito. Estos activos pueden incluir hardware, como computadoras y servidores, software, datos, propiedad intelectual, reputación de la Institución, capital humano, entre otros.

Recursos:	Pueden abarcar una amplia variedad de elementos, como personas, tecnología, tiempo, dinero, conocimiento, entre otros. Estos recursos son esenciales para llevar a cabo actividades, proyectos o procesos de una organización.
Información:	Es un recurso cuyo origen se genera al interior de la organización a través de los distintos procesos de negocio donde se registran, procesan y almacenan datos operacionales, comerciales y financieros. Todo este gran cúmulo de datos, denominados recursos de información, al igual que otros activos comerciales importantes, esenciales para la continuidad y, en consecuencia, necesita ser protegida adecuadamente.

VI. ÁMBITOS DE ACCIÓN

1. ADMINISTRACIÓN DE LOS RECURSOS INFORMÁTICOS Y TECNOLÓGICOS

1.1 Clasificación de Información

La Universidad Mayor establece la siguiente clasificación de los activos de información según su confidencialidad:

Clasificación de Confidencialidad de Activos de Información	
Restringido	Información de carácter privada de cualquier dato o conjunto de datos de propiedad o dominio de La Universidad Mayor, cuyo acceso está restringido y cuya divulgación no autorizada podría causar daño significativo a la organización.

Confidencial	Información que solo puede ser accedida por un número limitado de personas autorizadas o bajo autorización del responsable de la información y cuya divulgación podría generar impactos legales o financieros.
Uso Interno	Información que únicamente puede ser accedida o conocida por los empleados de La Universidad Mayor
Pública	Información sin restricciones de circulación que pueden ser conocidos o accedidos por cualquier individuo, ya sea interno o externo a La Universidad Mayor y cuya divulgación no causaría daño a la organización.

La Universidad Mayor establece las siguientes medidas de protección según la clasificación de la información:

- Para la información restringida, se aplicarán medidas de seguridad estrictas, como el cifrado de doble nivel, la autenticación multifactor o el control de acceso granular.
- Para la información confidencial se aplicarán medidas de seguridad como control de acceso.
- La información interna estará protegida por medidas de seguridad como firewalls, antivirus y segmentación de redes.
- La información pública estará accesible de forma segura a través de canales web o portales designados.

1.2 Uso adecuado de activos

Todos los trabajadores, alumnos y terceros que tengan acceso a los activos de información de la Universidad Mayor tienen la obligación de cumplir y apegarse estrictamente a las políticas de uso aceptable y eficiente de los recursos asignados. Esto implica un uso responsable, ético y transparente de los recursos de la Institución, velando siempre por su cuidado y preservación.

1.2.1 Tratamiento adecuado de la información

Es fundamental que todos los trabajadores resguarden la información confidencial de la Universidad Mayor. Es crucial evitar la divulgación de información sensible a personas no autorizadas, ya que esto podría acarrear graves perjuicios a la Institución, tanto en términos financieros como de reputación. Se debe tener especial cuidado al manejar datos sensibles, siguiendo los protocolos de seguridad establecidos y tomando las medidas necesarias para prevenir accesos no autorizados o filtraciones de información.

1.2.2 Uso de los sistemas y equipos de cómputo

Los sistemas informáticos (sean hardware, software y/o periféricos), así como la información contenida en ellos, son propiedad de la Institución y su uso está limitado exclusivamente a los fines comerciales de la misma. Cualquier utilización, alteración o acceso no autorizado a los sistemas dará lugar a acciones disciplinarias y/o legales correspondientes.

Sólo se permitirá la conexión de equipos y dispositivos de propiedad de la Institución a las redes institucionales y aquellos que cuenten con la autorización formal por parte de la Dirección de Tecnología, siempre y cuando cumplan con las medidas de seguridad establecidas, lo mismo aplica a las redes inalámbricas. No obstante, se permite el uso de redes inalámbricas para invitados, los cuales no tendrán conexión con la red institucional, pero permitirán el acceso a Internet. La Dirección de Tecnología de la información tomará medidas en respuesta al tráfico malicioso, incluyendo la posibilidad de prohibición o bloqueo de los equipos.

La Universidad Mayor se reserva el derecho de supervisar o controlar, en cualquier momento, el uso que los usuarios hacen de los recursos informáticos y de información proporcionados.

Queda estrictamente prohibida la modificación de la configuración de las políticas de seguridad establecidas por la institución.

1.2.3 Uso del correo electrónico

Las comunicaciones por correo electrónico entre la Institución y sus partes interesadas deben llevarse a cabo exclusivamente mediante el sistema de correo proporcionado por la Universidad Mayor. No se permite el uso de cuentas de correo personales para comunicarse con las partes interesadas de la organización, ni para transmitir cualquier información relacionada con el negocio.

La Universidad Mayor podrá monitorear o acceder a todos los medios electrónicos en forma aleatoria o de acuerdo con el procedimiento que se establezca con la finalidad de regular su correcto manejo y uso, detectar el incumplimiento de obligaciones referidas a su manejo o uso u otras de carácter laboral, todo ello de conformidad a su potestad de dirección y administración.

El buzón de correo asignado a cada usuario es personal e intransferible, y es responsabilidad del trabajador garantizar su seguridad protegiendo su contraseña de acceso. Además, es el único responsable del uso adecuado de su cuenta de correo, la cual está destinada exclusivamente para las necesidades de la Institución.

Se prohíbe enviar, distribuir o reenviar mensajes que atenten contra la dignidad, intimidad y reputación de personas o instituciones, así como realizar cualquier forma de acoso, difamación, calumnia o actividad hostil con la intención de intimidar o insultar. También está prohibido difundir ideas políticas, religiosas y propaganda, no se considerarán perturbaciones los mensajes enviados por el o los sindicatos o dirigentes sindicales en el ejercicio de su labor sindical, los que siempre estarán permitidos ya sea que emanen del correo dispuesto por la Institución o de otro creado con la finalidad.

Los trabajadores no pueden enviar mensajes anónimos, literatura variada, encuestas, concursos, esquemas piramidales, cartas en cadena, mensajes no solicitados o cualquier conducta reprochable en el ámbito laboral y penal.

Se insta a los trabajadores de la Universidad Mayor a evitar el envío desde su buzón elementos (textos, softwares, música, imágenes u otros) que infrinjan la legislación vigente y los reglamentos internos sobre propiedad intelectual y derechos de autor, incluyendo los de la institución.

Es responsabilidad de los trabajadores gestionar de manera eficiente el contenido de sus carpetas de correo electrónico. Deben eliminar periódicamente los mensajes innecesarios para evitar que permanezcan por tiempos prolongados, lo que podría aumentar el uso de recursos y ocasionar congestión, afectando la capacidad de recibir nuevos mensajes. Este proceso debe realizarse siguiendo los procedimientos establecidos por la Universidad Mayor para la eliminación de correos electrónicos, asegurando el cumplimiento de las políticas de seguridad de la información y controles de protección de datos.

1.2.4 Navegación en Internet

Los trabajadores, contratistas y terceras partes deben abstenerse de descargar programas que realicen conexiones automáticas o visores de sitios cuyo contenido atente contra los valores de la Institución o la regulación vigente, clasificados como pornografía, drogas, terrorismo, religiosos y/o étnicos, así como la utilización de recursos para distribución o reproducción de este tipo de material.

Queda estrictamente prohibido la descarga de software desde internet hacia los equipos de la organización, a menos que sea expresamente autorizado por el Director de Tecnología de la Información (Chief Information Security Officer).

Los trabajadores no deben recopilar, almacenar, divulgar, transmitir o solicitar cualquier material, información, mensaje o comunicación que pueda infringir o violar patentes, derechos de autor, marcas, secretos Institucionales u otros derechos de propiedad intelectual de terceros, programas de computación dañinos, virus y/o software malicioso en general. La Universidad Mayor se reserva el derecho de monitorear y/o registrar toda información entrante y saliente a través de la conexión a internet de la institución.

Asimismo, la institución se reserva el derecho de filtrar el acceso a contenidos no autorizados desde su red corporativa, prohibiendo el ingreso a páginas relacionadas con abuso de drogas, alcohol, hacking, actividades ilegales o no éticas, discriminación, violencia explícita, grupos extremistas, proxies anónimos, navegación de incógnito, navegación en la dark web, plagio, abuso de menores, pornografía, venta de armas, sitios de descarga, sitios de almacenamiento no autorizados, conexiones P2P, phishing, spam, propaganda, entre otros.

Para acceder a aplicaciones, sistemas o equipos internos utilizados o respaldados por personas que se conecten remotamente desde internet, se deben emplear conexiones seguras que incluyan elementos de seguridad como doble factor de autenticación, cifrado de las comunicaciones y mecanismos de prevención de pérdida de datos (DLP).

La Dirección de Tecnología tiene la responsabilidad de establecer las reglas de control de acceso de acuerdo con las necesidades del negocio. Cualquier excepción a estas reglas debe ser autorizada por Director de Tecnologías de la Información.

1.2.5 Uso de herramientas que comprometen la seguridad.

No está permitido hacer o intentar hacer, cualquiera de los siguientes actos:

- Monitorear datos o tráfico en las redes de la institución sin la debida autorización del usuario o administrador de la red.
- Sondear, copiar, probar firewalls o herramientas de hacking.
- Cargar archivos que contengan virus, troyanos, gusanos, archivos dañados o cualquier otro programa o software similar que pueda perjudicar el funcionamiento de los equipos de la red.
- Atentar contra la vulnerabilidad del sistema o redes de la institución.
- Realizar ataques de denegación de servicio sobre los sistemas y redes de la institución.
- Violar las medidas de seguridad o las rutinas de autenticación del sistema o de la red.
- Cualquier actividad que intente la recopilación de información de cualquier equipo o sistema con propósitos no establecidos ni acordados previamente.

1.2.6 Recursos compartidos

Queda prohibido el uso compartido de carpetas en computadoras personales. Los usuarios que lo requieran podrán utilizar carpetas compartidas centralizadas definidas por la Dirección de Tecnologías de la Información en el servidor de archivos de usuario o en un servicio de directorios compartidos en la nube.

Esto presenta la ventaja adicional de que la información almacenada en estos recursos está respaldada en las copias de respaldo de datos.

El acceso a estos recursos compartidos solo se otorgará con la autorización del responsable de la información contenida en la carpeta y/o de la Dirección de Tecnología.

El acceso a carpetas compartidas debe restringirse a los usuarios que las necesiten.

No se permitirá el acceso a estas carpetas a usuarios que accedan desde equipos que no cuenten con el antivirus corporativo.

1.2.7 Uso de equipos portátiles y dispositivos móviles

El uso de equipos portátiles conlleva riesgos asociados al posible robo o pérdida, lo cual puede comprometer la información almacenada o accesible desde dichos dispositivos.

Los trabajadores, que utilicen equipos portátiles y dispositivos móviles de propiedad de la Universidad Mayor se comprometen a seguir las siguientes directrices:

- Proteger físicamente los dispositivos móviles (notebooks, laptops y smartphones) proporcionados por la Institución contra el uso indebido, robo o pérdida, especialmente en automóviles, habitaciones de hotel, centros de formación, reuniones, cafeterías, etc. No se deberá dejar sin vigilancia un equipo que contenga información importante, sensible o crítica; siempre que sea posible, se deberá dejar bajo llave.
- Utilizar técnicas de encriptación para prevenir el acceso no autorizado o la divulgación de información almacenada en estos dispositivos.
- Asegurarse de que la información sensible almacenada en los dispositivos móviles tenga copias de seguridad recuperables en caso de pérdida o robo del dispositivo.
- Configurar el equipo móvil para bloquearse automáticamente después de un periodo de inactividad, con opciones de desbloqueo como contraseña, reconocimiento de voz, entre otras.

- Comprometerse al uso de aplicaciones antivirus y a utilizar canales seguros y cifrados y no conectarse a redes compartidas de acceso libre, no seguras.

La Dirección de Tecnología es responsable de mantener un registro e inventario de los equipos móviles de la institución.

Únicamente se autoriza el acceso a la información de la Institución, el uso de servicios de información y recursos de la Institución para equipos y dispositivos móviles de propiedad de la Universidad Mayor que cumplan con el estándar de seguridad definido, así como con los mecanismos de autenticación establecidos.

Los trabajadores de la Universidad Mayor que utilicen equipos móviles deben adoptar buenas prácticas y contar con estándares de configuración para proteger dichos activos. Cada persona responsable de un equipo móvil asumirá la responsabilidad y consecuencias que puedan surgir debido al uso indebido, accesos no autorizados, descuidos, pérdidas de confidencialidad y/o robo.

Sólo se permitirán aplicaciones autorizadas por la Institución en los equipos móviles que sean de su propiedad, y los usuarios tienen prohibido instalar aplicaciones no autorizadas. Cualquier aplicación adicional requerida y no incluida en el listado autorizado debe ser aprobada por la Dirección de Tecnología de la Información, y se debe mantener un registro escrito de esta.

La Dirección de Tecnología establecerá e implementará el estándar de seguridad de la información para equipos y dispositivos móviles, realizará revisiones periódicas para garantizar su cumplimiento y mantendrá el registro de equipos entregados y sus usuarios.

Los equipos y dispositivos móviles deben contar con mecanismos de protección contra software malicioso según el estándar definido por la Dirección de Tecnología.

Los responsables de equipos portátiles y dispositivos móviles de propiedad de la institución deben informar a la Dirección de Tecnología en caso de pérdida, robo u otros eventos, quienes deben llevar a cabo la inhabilitación, borrado de información y bloqueos necesarios y oportunos para evitar la pérdida de confidencialidad de la información contenida en el equipo o dispositivo.

Además, los responsables de equipos y dispositivos móviles de propiedad de la institución deben utilizar los recursos establecidos por la organización para el respaldo adecuado de la información del negocio.

1.3 Notificación de Incidentes de Seguridad y Situaciones de Riesgo

Todos los trabajadores de la Universidad Mayor tienen la responsabilidad de informar cualquier incidente, vulnerabilidad o infracción de seguridad que comprometa a equipos de la institución, o a equipos propios que tengan acceso a la información de la institución, a la Dirección de Tecnología de la Información lo que contribuirá a que la organización gestione adecuadamente el incidente y minimice su impacto en el conjunto de la Institución.

1.4 Acceso remoto

Solo el personal autorizado tiene permitido acceder de forma remota a la red de la Universidad Mayor y a sus sistemas. Este acceso debe llevarse a cabo exclusivamente a través de un mecanismo de comunicación que integre sistemas de autenticación y encriptación de las comunicaciones. En particular, se emplearán conexiones mediante red privada virtual (VPN) gestionadas por el sistema firewall de la dirección de tecnologías de la información, así como otros métodos que garanticen comunicaciones seguras.

Los dispositivos habilitados para conectarse de esta manera deben cumplir con los requisitos y configuraciones, lo que incluye la instalación del antivirus corporativo.

1.5 Equipo de usuario desatendido

Es necesario que los usuarios bloqueen la sesión en sus equipos cada vez que se ausenten de sus estaciones de trabajo.

Para garantizar la seguridad, todos los equipos de escritorio, portátiles y dispositivos móviles que accedan a los recursos de la organización deben contar con el bloqueo de sesión después de un periodo de 15 minuto de inactividad.

Además, se requiere que todos los equipos de escritorio, portátiles y dispositivos móviles soliciten las credenciales de acceso al usuario cada vez que se enciendan, reinicien, suspendan o bloqueen la sesión, asegurando así una capa adicional de seguridad.

1.6 Puesto de trabajo despejado y pantalla limpia

Cuando los usuarios necesiten ausentarse de sus estaciones de trabajo, es imperativo que, además de bloquear su equipo, guarden de manera segura cualquier información física (documentos) y/o lógica (medios magnéticos u ópticos removibles) que contengan información clasificada como confidencial, ya sea propia o de clientes de la universidad.

Es fundamental que los equipos de reproducción de información, tales como impresoras y fotocopiadoras, estén ubicados en lugares con acceso controlado para garantizar una mayor seguridad en el manejo de la información confidencial.

1.7 Transferencia de información

La transferencia de información entre nuestra institución y terceros mediante el uso de software o herramientas no autorizadas por la Dirección de Tecnologías de la Información está estrictamente prohibida. Solo se permite el uso de canales de comunicación y transferencia de datos, tales como:

- Correo electrónico corporativo.
- Plataformas corporativas de almacenamiento en la nube.
- Herramientas corporativas de colaboración en línea.
- Portales y sistemas corporativos.

Cualquier intercambio de información confidencial entre la Universidad y terceros debe respaldarse siempre con un contrato firmado por ambas partes. Este contrato debe incluir una cláusula de confidencialidad y no divulgación de información, o al menos, debe existir un acuerdo de confidencialidad con el mismo propósito.

1.8 Restricciones de instalación y uso de software

Los trabajadores y contratistas no cuentan con la autorización para descargar e instalar software de cualquier tipo en los equipos de la organización.

En situaciones donde el negocio requiera el uso o instalación de software, los jefes de cada área deben solicitar la instalación del software a la dirección de tecnologías de la información, la cual tiene la facultad de autorizar o rechazar la solicitud de instalación, así como gestionar el pago por el uso del software.

Cabe destacar que la Dirección de Tecnologías de la Información es la única entidad autorizada para llevar a cabo la descarga e instalación de software en los equipos de la organización, siempre sujeta a la previa autorización.

VII. UNIDAD(ES) A CARGO

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

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