Universidad Mayor | Dirección de Tecnologías de la Información

POLÍTICA DE CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN Y SISTEMAS INFORMÁTICOS

POLÍTICA DE CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN Y SISTEMAS INFORMÁTICOS[1]

I. OBJETO

El objeto de la presente Política es proteger los sistemas y datos de la Universidad Mayor contra accesos no autorizados y garantizar que los usuarios tengan acceso solo a los recursos necesarios para realizar sus tareas laborales, previniendo el acceso no autorizado a sistemas de información y servicios informáticos de la organización.

Se debe asegurar que los usuarios sean responsables de sus acciones en los sistemas de la Institución, a su vez que se garantiza el adecuado funcionamiento del Sistema de Gestión de Seguridad de Información (SGSI) y su mejora continua.

II. ALCANCE

Esta política se aplica a todos los trabajadores, contratistas y terceros que acceden a los sistemas de información y datos de la universidad que cuenten con un usuario de acceso a una plataforma tecnológica. Donde se dictan pautas sobre los requisitos y prácticas de control de acceso lógico a las redes, sistemas y aplicaciones, así como las responsabilidades de los usuarios en relación con el uso de tales recursos.

Esta política se aplica a todos los sistemas y datos de la institución, incluyendo redes, servicios de red, sistemas y aplicaciones.

III. DECLARACIÓN INSTITUCIONAL

La Universidad Mayor reconoce que el control de accesos constituye un pilar fundamental para la protección de sus activos de información, la continuidad de sus procesos y el cumplimiento de las obligaciones normativas vigentes.

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

Documento Controlado, prohibida su reproducción parcial o total sin autorización

En este sentido, declara su compromiso de implementar y mantener mecanismos que garanticen que cada usuario acceda únicamente a los recursos estrictamente necesarios para el desempeño de sus funciones, bajo el principio de privilegio mínimo.

Asimismo, la Universidad establece lineamientos claros para regular la creación, modificación y eliminación de accesos, promoviendo el uso responsable de credenciales, la aplicación de mecanismos de autenticación robusta y la revisión periódica de privilegios. Con ello se busca prevenir accesos indebidos, reducir riesgos de exposición o pérdida de información y fomentar una cultura institucional de seguridad, confidencialidad y responsabilidad compartida en el manejo de los sistemas y servicios tecnológicos.

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

V. DEFINICIONES

Para efectos de la presente Política se entenderá por:

Concepto	Descripción
Acceso:	Proceso mediante el cual se permite o deniega a un usuario o entidad la entrada o utilización de recursos, sistemas o áreas específicas.

Altas, Bajas y Modificaciones:	Proceso de agregar, eliminar o modificar permisos específicos relacionados con la gestión de permisos y derechos de acceso.
Contraseña:	Clave secreta utilizada para autenticar y verificar la identidad de un usuario antes de permitirle acceder a sistemas, aplicaciones o recursos.
Gestión de acceso:	Prácticas y procedimientos utilizados para administrar y regular el acceso a sistemas, recursos y áreas dentro de una organización.
Gestión de privilegios de acceso:	Se refiere a las prácticas y procedimientos utilizados para administrar y regular los derechos y permisos otorgados a los usuarios en sistemas, aplicaciones y recursos.

VI. ÁMBITOS DE ACCIÓN

1. Acceso a redes y servicios de red

El acceso a las redes y servicios de red se otorgará solo a los usuarios que necesiten de este acceso para realizar sus tareas laborales. Se otorgará en función del principio de “necesidad mínima”, lo que significa que los usuarios sólo tendrán acceso a los recursos necesarios para realizar sus tareas laborales.

Solamente tendrán acceso y podrán utilizar los sistemas de información aquellas personas o entidades que tengan un vínculo contractual con la universidad, así como los trabajadores y contratistas que requieran dicho acceso para el desarrollo de sus funciones, cuyo particular será analizado y aprobado por el director de tecnología de la información.

Es importante que las conexiones a los servicios de red sean seguras, tanto internas como externas. Si no se toman medidas para garantizar la seguridad de estas conexiones, toda la organización puede verse afectada. Por lo tanto, se controlará el acceso a los servicios de red para evitar que los usuarios comprometan la seguridad de la red y sus servicios.

Para garantizar la seguridad de los equipos informáticos de escritorio (desktop) y/o portátiles (laptop), es importante que todos los trabajadores que ingresen a sus cuentas de usuario estándar sin privilegios. Esto

Documento Controlado, prohibida su reproducción parcial o total sin autorización

significa que no tendrán acceso a todas las funciones del equipo, pero podrán realizar sus tareas diarias sin comprometer la seguridad de la información.

Todos los trabajadores, proveedores y contratistas que trabajan en la institución pueden acceder a los sistemas de información, servicios y recursos de la organización. Sin embargo, para garantizar la seguridad de la información, es importante que estos accesos se realicen únicamente a través de la infraestructura de la red cableada o inalámbrica, o conexiones remotas seguras previamente autorizadas por la Dirección de Tecnologías de la Información.

Solo el personal técnico es responsable de administrar dichos activos, cualquier otro usuario que debido a que sus labores requieran tener acceso a cuentas de usuario con privilegios especiales, deben ser autorizados por el director de tecnología de la información.

Para garantizar la seguridad de la información, es importante que los trabajadores, proveedores y contratistas que presten servicio en la universidad, se autentiquen en los sistemas de información y servicios. Esto se hace mediante el uso de un código de usuario y contraseña, que ayuda a validar que la persona que intenta acceder es quien dice ser y al menos un factor adicional de autenticación.

La Dirección de Tecnologías de la Información, en conjunto con su director, definirá los mecanismos de autenticación que se utilizarán.

1.1 Gestión de acceso para Altas, Bajas y Modificaciones

La gestión de acceso para Altas, Bajas y Modificaciones se realizará de acuerdo con los procedimientos establecidos por la institución. Los cambios en los permisos de acceso se realizarán solo después de la aprobación de quién corresponda.

Para garantizar la seguridad de la información, es importante que todos los usuarios que ingresen a los sistemas de información y/o servicios de la organización tengan un identificador de usuario único (ID) que les identifique durante el uso y acceso a los sistemas de información.

Documento Controlado, prohibida su reproducción parcial o total sin autorización

La Dirección de Tecnologías de la Información es responsable de asignar identificadores de usuario únicos, entregar credenciales de acceso temporales de forma segura y obligar a los usuarios a cambiar dichas credenciales durante su primer inicio de sesión. También es responsable de suspender y/o ajustar los accesos a las aplicaciones internas, servicios y demás recursos tecnológicos a través del bloqueo de usuarios o ajustes de sus privilegios de acceso, para aquellos usuarios que por decisión propia o de la organización hayan finalizado el vínculo contractual, o en aquellos casos en que, por el desarrollo de actividades, se requiera un cambio de permisos.

Si algún trabajador y/o terceros requieren de derechos de accesos adicionales a los establecidos, deben solicitarlos a través del procedimiento formal de control de acceso y los mismos podrán ser otorgados solo luego de haber sido autorizados. Los responsables de los activos de información serán los encargados de autorizar los permisos solicitados por un usuario determinado (sujeto a la aprobación de su jefatura interna), previo a la asignación de dichos permisos por parte de la Dirección de Tecnología.

Además, se debe mantener un control y registro único y centralizado de los accesos otorgados que identifica: el código de cada usuario, los permisos de acceso otorgados a los distintos sistemas y recursos, la fecha del otorgamiento, quién solicita, quién autoriza y quién suministra los accesos aprobados.

Se realizarán auditorías internas o externas al menos una vez al año para revisar que los usuarios que acceden a los activos estén autorizados y tengan los privilegios apropiados. La Dirección de Tecnologías de la Información debe llevar un control de los permisos de acceso y privilegios de acceso sobre los usuarios que han tenido cambio de responsabilidades o han sido desvinculados de la organización.

1.2 Gestión de privilegios de accesos

Los privilegios de acceso se otorgarán en función del principio de “necesidad mínima”, lo que significa que los usuarios sólo tendrán acceso a los recursos necesarios para realizar sus tareas laborales. Los privilegios de acceso se revisarán periódicamente para garantizar que los usuarios tengan acceso solo a los recursos necesarios.

Documento Controlado, prohibida su reproducción parcial o total sin autorización

Para garantizar la seguridad de la información, es importante que todos los usuarios que acceden a los sistemas de información, servicios y recursos de la universidad, tengan el mínimo privilegio de acceso posible para realizar sus funciones y desarrollar el negocio.

Todos los trabajadores, proveedores y contratistas que accedan a los equipos informáticos de escritorio y/o portátiles deberán ingresar bajo el tipo de cuentas de usuario estándar sin privilegios, a excepción del personal técnico de la Dirección de Tecnologías de la Información, quienes son responsables de administrar dichos activos, y otros usuarios que sean explícitamente autorizados para ello.

Los trabajadores, proveedores y contratistas que cuenten con un código de usuario privilegiado, únicamente deberán hacer uso de estos para los fines para el cual fueron autorizados y abstenerse de ejecutar desde el mismo las actividades normales del negocio. Todas las contraseñas de cuentas de altos privilegios (root, administradores, cuentas de administración de aplicaciones, cuentas de administración del correo electrónico, etc.) deben ser cambiadas al menos una vez cada 3 meses.

La Dirección de Tecnologías de la Información es responsable de resguardar la confidencialidad de la información de autenticación secreta (contraseña) del o los usuarios administradores de los sistemas de información, servicios y recursos sobre los cuales acceden y administran.

Es importante que el personal técnico, que resguarde los códigos de usuario, administrador(es) y la(s) información(es) de autenticación secreta (contraseña) de acceso a los sistemas de información, servicios y recursos de la organización, documente y haga entrega formal de la información al trabajador directamente.

1.3 Gestión de las contraseñas

Para garantizar la seguridad de la información, es importante que todos los trabajadores, proveedores y contratistas cambien sus contraseñas de acceso de forma periódica, como mínimo cada 3 meses. Además, es importante que las contraseñas sean seguras y de calidad.

Para cumplir con estos requisitos, las contraseñas de los sistemas que trabajen con MFA deben tener al menos:

Documento Controlado, prohibida su reproducción parcial o total sin autorización

- 8 caracteres.
- Utilizar caracteres de tres de los cuatro grupos siguientes. Al menos uno de los caracteres debe ser un símbolo:
    - Letras minúsculas.
    - Letras mayúsculas.
    - Números (por ejemplo, 1, 2, 3).
    - Símbolos (por ejemplo, ¡, @, Ñ, =\`{}[]:";'<>?,./).

Las contraseñas de los sistemas que no cuenten con MFA deben tener al menos:

- 14 caracteres.
- Utilizar caracteres de tres de los cuatro grupos siguientes. Al menos uno de los caracteres debe ser un símbolo:
    - Letras minúsculas.
    - Letras mayúsculas.
    - Números (por ejemplo, 1, 2, 3).
    - Símbolos (por ejemplo, ¡, @, Ñ, =\`{}[]:";'<>?,./).
- Las claves utilizadas para el primer acceso al sistema deben ser exclusivas y seguras, y deben ser comunicadas al usuario de forma segura, verificando previamente la identidad del usuario. Debe dejarse constancia de la recepción de la clave por parte del usuario receptor.
- Además, es importante que los usuarios cambien sus contraseñas luego del primer inicio de sesión exitoso y que se mantenga un histórico de contraseñas usadas, evitando la reutilización de al menos

Documento Controlado, prohibida su reproducción parcial o total sin autorización

las 3 últimas. Las contraseñas deben almacenarse encriptadas con un algoritmo seguro no reversible y transmitirse de forma segura.

Todos los sistemas que utilicen contraseñas como método de autenticación de usuario deberán implementar las siguientes características de funcionamiento:

- Al ingresar la contraseña ésta no debe ser desplegada.
- En caso de cinco intentos de autenticación fallidos continuados, el sistema debe bloquear la cuenta.

1.4 Responsabilidad de los usuarios

Los usuarios son responsables de proteger sus credenciales de acceso y de utilizar los sistemas y datos de manera responsable. Los usuarios deben informar cualquier sospecha de acceso no autorizado o actividad sospechosa a su jefatura de inmediato.

Es importante que cada trabajador, proveedor y contratista proteja la confidencialidad de su información de autenticación secreta (contraseña). Si la pierde, roban o existe la sospecha que alguien más conoce la contraseña, es responsabilidad de cada uno reportarlo a través de los canales de comunicación oficiales.

Las cuentas con privilegios de administrador no deben utilizarse para actividades cotidianas como la navegación en Internet, el acceso al correo electrónico o el uso de aplicaciones ofimáticas, ya que estas prácticas incrementan el riesgo de comprometer credenciales críticas. Todo administrador de sistemas debe disponer una cuenta de usuario nominal con el mínimo privilegio para las labores diarias. El uso de cuentas de administrador con privilegios amplios debe estar estrictamente limitado, debidamente controlado y siempre justificado.

El acceso a los sistemas sólo podrá efectuarse desde dispositivos provistos por la universidad para tales efectos, salvo algunas excepciones, autorizadas y controladas de las personas autorizadas por la Dirección de Tecnologías de la Información, sin perjuicio de que la responsabilidad de protección, resguardo y confidencialidad de las credenciales y accesos es siempre del trabajador.

Documento Controlado, prohibida su reproducción parcial o total sin autorización

No está permitido escribir y/o almacenar la información de autenticación secreta (contraseña) en papeles, post-it, ficheros o archivos digitales no protegidos, entre otros mecanismos que permitan su divulgación. Tampoco está permitida la divulgación de la información de autenticación secreta (contraseña) a través de ningún medio, así como el préstamo y uso compartido de códigos de usuario y contraseñas. A este efecto, está prohibido incluir contraseñas en mensajes de correo electrónico, ni ningún otro medio de comunicación electrónica. Tampoco deben ser comunicadas las contraseñas en conversaciones telefónicas. La contraseña no debe comunicarse ni a superiores ni a subalternos, compañeros de trabajo, amigos, familiares o a cualquier persona.

Es importante que cada trabajador, proveedor y contratista proteja la confidencialidad de su información de autenticación secreta (contraseña). Si un colega asume algunas de las tareas de un trabajador ausente, en ningún caso el trabajador debe compartir su código de usuario y contraseña con él. Si el colega requiere accesos equivalentes al trabajador ausente, su jefatura deberá solicitarlos a través de los procedimientos definidos para ello.

No está permitido utilizar la opción “recordar claves” sobre los programas a través de los cuales se accede a los sistemas de información y servicios. Todos los trabajadores y/o contratistas son responsables de cambiar la clave de acceso a los sistemas de información y servicios de forma periódica.

La asignación de códigos de usuario y contraseña para acceder a la red y aplicaciones debe ser realizada de forma individual. No está permitido el uso de códigos de usuario y contraseñas compartidas. Todos los códigos de usuario asignados a los trabajadores, proveedores y contratistas deben bloquearse de forma preventiva tras un límite de intentos fallidos durante el inicio de sesión de su cuenta.

Los trabajadores, proveedores y contratistas deben hacer uso de contraseñas seguras para el acceso a los sistemas de información, servicios y recursos de la organización, según lo descrito en el punto 4 de este documento, y siguiendo las recomendaciones a continuación:

- No utilizar contraseñas que se puedan adivinar fácilmente, como pueden ser:

  — Una cadena de caracteres derivada del nombre de la cuenta del usuario.

Documento Controlado, prohibida su reproducción parcial o total sin autorización

- Una cadena de caracteres formada por la repetición de caracteres.
- Una palabra contenida en un diccionario (de lengua española o extranjera).
- Una palabra de diccionario seguida o precedida de un carácter (por ej.: “palabra1” o “Xpalabra” o “palabra!”).
- Un nombre de pila: Nombres de familiares, amigos, mascotas, ciudades, etc.
- Fechas de cumpleaños u otra información personal tales como dirección o número de teléfono.
- Conjuntos de letras o números que sigan un patrón sencillo, tales como aaabbb, qwerty, abcdef, 123321, etc.

Una clave no debe ser una palabra que se encuentre en el diccionario, en un dialecto o jerga de ningún idioma, como tampoco ninguna de estas palabras escritas hacia atrás.

Es importante crear contraseñas que se pueda fácilmente recordar. Una forma de hacerlo es crear una contraseña basada en una frase recordable.

1.5 Control de acceso a sistemas y aplicaciones

El acceso a los sistemas y aplicaciones se otorgará solo a los usuarios que necesiten acceso para realizar sus tareas laborales. El acceso se otorgará en función del principio de “necesidad mínima”.

Es importante que los sistemas y aplicaciones implementen mecanismos de control de acceso que validen a los usuarios autorizados y establezcan derechos de acceso de acuerdo con los perfiles de usuario definidos.

La Dirección de Tecnologías de la Información es responsable de implementar los cambios previamente aprobados en la estructura de los perfiles de usuario en los sistemas. Estas estructuras delimitan las acciones permitidas a ejecutar por los usuarios que acceden a los sistemas de información, controlan el acceso a los datos, los privilegios de acceso de los usuarios (lectura, escritura, borrado y edición) y la información obtenida en las salidas de los sistemas de información.

Documento Controlado, prohibida su reproducción parcial o total sin autorización

1.6 Control de acceso a instalaciones

El acceso a las instalaciones de la Universidad ya sea en los campus u otros establecimientos, está regido por el Protocolo de Control de Acceso Campus Seguro, el cual establece lineamientos generales para resguardar la seguridad de las personas, los bienes y la infraestructura crítica de la institución.

En este marco, el acceso al Datacenter de la Universidad está exclusivamente reservado para el personal autorizado que forma parte de las dependencias directamente vinculadas con su operación y administración. Se prohíbe de manera expresa el ingreso al público general y a cualquier persona que no cuente con autorización formal otorgada por la Dirección de Tecnologías de la Información (DTI). Esta medida busca proteger los activos de información y la infraestructura tecnológica que soporta las funciones académicas y administrativas.

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.

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

Documento Controlado, prohibida su reproducción parcial o total sin autorización