Universidad Mayor | Dirección de Tecnologías de la Información

POLÍTICA DE GESTIÓN DE COMUNICACIONES Y OPERACIONES (TI)

POLÍTICA DE GESTIÓN DE COMUNICACIONES Y OPERACIONES (TI)[1]

I. OBJETO

El objetivo principal de esta política es asegurar la gestión eficaz y segura de las comunicaciones y operaciones dentro de la organización, promoviendo prácticas seguras y mitigando los riesgos de seguridad cibernética para garantizar la continuidad de la operación.

II. ALCANCE

Esta Política se aplica a todos los trabajadores o subcontratistas de la Universidad Mayor que interactúan con los activos de la organización y participan en la gestión, monitoreo y operación de sistemas informáticos, comunicaciones, operaciones físicas y procesos operativos, entendiéndose por tales:

a. Activos de información: Toda la información generada, recibida, procesada, transmitida o almacenada por la organización, independientemente de su formato o soporte (físico o digital).
b. Equipos: Computadores personales, laptops, servidores, dispositivos móviles, equipos de comunicación, etc.
c. Plataformas de servicios informáticos: Sistemas operativos, software de aplicación, bases de datos, correo electrónico, internet, etc.

III. DECLARACIÓN INSTITUCIONAL

La Universidad Mayor reconoce la importancia estratégica de los activos de información, los equipos tecnológicos y las plataformas de servicios informáticos, entendidos como recursos esenciales para el desarrollo de sus funciones académicas, administrativas y de gestión.

En este sentido, 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 y a la continuidad operativa de los procesos críticos.

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

Documento Controlado, prohibida su reproducción parcial o total sin autorización

A través de esta Política, la Universidad se compromete a:

1. Proteger la confidencialidad, integridad y disponibilidad de la información y de los recursos tecnológicos que la soportan.
2. Promover un uso ético, transparente y conforme a la legislación vigente de los sistemas, servicios y plataformas institucionales.
3. Establecer lineamientos claros y controles técnicos y organizativos que permitan prevenir riesgos, reducir vulnerabilidades y mitigar incidentes de seguridad.
4. Fomentar una cultura institucional de resguardo y responsabilidad compartida, en la cual todos los miembros de la comunidad universitaria participen activamente en la protección 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.

Documento Controlado, prohibida su reproducción parcial o total sin autorización

V. DEFINICIONES

Para efectos de la presente Política se entenderá por:

Concepto	Descripción
Comunicaciones:	Se refiere a la transmisión de información entre diferentes partes interesadas, ya sea de forma verbal, escrita o electrónica.
Información:	Recurso que 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.
Firewall:	Sistema de seguridad que actúa como una barrera entre una red privada y otras redes externas, como Internet. Su función principal es controlar y filtrar el tráfico de datos según un conjunto de reglas predeterminadas.
Malware:	Se refiere a cualquier tipo de software diseñado con la intención de dañar, infectar o comprometer un sistema informático, red o dispositivos. Puede incluir virus, gusanos, troyanos, spyware, adware y otros tipos de programas maliciosos.

VI. ÁMBITOS DE ACCIÓN

1 GESTIÓN DE LAS COMUNICACIÓNES

1.1 Transferencia de información

La Universidad Mayor está comprometida a proteger la confidencialidad e integridad de la información durante su transferencia o intercambio con personal interno, externo, proveedores y clientes. Solo se permite el uso de canales de comunicación y transferencia de datos, tales como:

- Correo electrónico Institucional.

Documento Controlado, prohibida su reproducción parcial o total sin autorización

- Plataformas Institucionales de almacenamiento en la nube.
- Herramientas Institucionales de colaboración en línea.
- Portales y sistemas Institucionales.

Además, se implementarán medidas de seguridad necesarias para garantizar un intercambio de información seguro.

Se establecerán y formarán Contratos o Acuerdos de Confidencialidad y/o Intercambio de Información con las partes externas involucradas en dicho intercambio. Estos contratos o acuerdos deberán cumplir con los requisitos establecidos en la Política de Gestión de Seguridad de la Información para Proveedores.

El Director de Tecnologías de la Información tiene la responsabilidad de aprobar el formato de Acuerdo de Confidencialidad y/o de Intercambio de Información entre Universidad Mayor y las partes externas, donde se incluyen los compromisos asumidos y las obligaciones regulatorias relacionadas con posibles incumplimientos. Entre los aspectos a considerar, se debe incluir la prohibición de divulgar información proporcionada por la Universidad a terceros involucrados, así como la disposición de destruir dicha información una vez cumplido su cometido.

La Dirección de Tecnologías de la Información tiene la responsabilidad de definir los procedimientos y tecnologías necesarias para llevar a cabo el intercambio de información con clientes y proveedores de Universidad Mayor. Asimismo, se deben implementar controles adecuados para asegurar y proteger los principios de seguridad de la información durante dicho intercambio.

El Director de Tecnología de la Información debe garantizar el cumplimiento de los lineamientos de Seguridad de la Información establecidas en este documento, y supervisar que los procedimientos se apliquen adecuadamente en las interacciones de la Universidad con sus proveedores, entidades relacionadas y clientes externos.

La Dirección de Tecnología de la Información es responsable de desplegar y mantener los servicios y herramientas seguras destinadas al intercambio de la información.

Documento Controlado, prohibida su reproducción parcial o total sin autorización

1.2 Seguridad de las Comunicaciones

La Dirección de Tecnología tiene a su cargo la gestión, protección y mantenimiento de los equipos de tecnología y comunicaciones en la Universidad Mayor. Cualquier modificación en la red debe ser debidamente registrada y fundamentada.

Universidad Mayor implementará los controles necesarios para asegurar la disponibilidad de los datos y de los servicios que dependen de ellos. Además, se asegurará de disponer de las medidas de seguridad adecuadas para proteger la integridad y confidencialidad de la información transmitida.

La Dirección de Tecnologías de la Información tiene la tarea de definir los dominios de seguridad adecuados para regular el acceso y control de la red de comunicaciones de la institución por parte del personal de la Universidad Mayor y/o terceros autorizados. Además de organizar las redes de datos segmentadas en grupos de acuerdo con lo considerado pertinente para la organización y definir los estándares técnicos para la configuración de los dispositivos de seguridad y de red en la infraestructura tecnológica de la Universidad Mayor, adoptando prácticas recomendadas para asegurar una configuración segura de estos dispositivos.

Asimismo, es responsable de identificar, justificar y registrar los servicios, protocolos y puertos que la organización autoriza en sus redes de datos, y proceder a deshabilitar o suprimir cualquier otro servicio, protocolo o puerto que no sea necesario.

El manejo de la red de comunicaciones de la Universidad requiere ser supervisado y aprobado, asegurando que cada intento de acceso ya sea exitoso o fallido, sea considerado para su análisis.

Cualquier usuario que se conecte a la red interna de comunicaciones de la Universidad debe poseer una identificación única que facilite su reconocimiento dentro de la red. Cada petición para establecer conexiones internas (tales como FTP, VPN´s y similares) hacia el dominio de Universidad Mayor requiere ser formalmente presentada, justificada por el solicitante, aprobada por la gerencia que la solicita y está sujeta a validación de la dirección de tecnologías de la información.

Documento Controlado, prohibida su reproducción parcial o total sin autorización

Se deben realizar auditorías de revisiones regulares para verificar el cumplimiento de los controles establecidos y presentar informes correspondientes a la dirección de Contraloría.

Nuestra institución establecerá los protocolos de seguridad y los servicios de red esenciales para la defensa de la red de datos, comprometiéndose a integrar estos requerimientos en los contratos de servicios de red cuando se externalicen.

1.3 Política de Firewall

Las configuraciones de firewalls deben restringir exclusivamente las conexiones establecidas en la red interna, denegando cualquier conexión entrante no asociada con una sesión previamente establecida. Los firewalls deben implementar mecanismos de detección y prevención de intrusiones, así como accesos no autorizados.

Cada conexión de Internet entrante y saliente debe contar con una configuración de firewall que permita a la organización supervisar, controlar el acceso y minimizar las posibilidades de acceso no autorizado a la red interna.

Para prevenir la manipulación de direcciones IP y evitar su ingreso a la red, la configuración de los firewalls debe incorporar medidas anti-suplantación.

Se requiere una administración general del firewall, identificando claramente los participantes, sus roles y responsabilidades. Cualquier modificación en un firewall debe ajustarse al proceso de control de cambios.

Cada regla de firewall que permita un tipo específico de tráfico o puerto debe respaldarse con una justificación de negocio. El uso de puertos o protocolos no justificados debe bloquearse al tráfico.

La configuración de los firewalls de acceso a Internet debe incorporar filtros de contenido, definiendo las categorías permitidas o prohibidas mediante el Comité de Ciberseguridad.

Documento Controlado, prohibida su reproducción parcial o total sin autorización

2 GESTIÓN DE LAS OPERACIONES

2.1 Copias de respaldo

La Universidad lleva a cabo la creación de copias de seguridad y el almacenamiento de su información crucial, asignando los recursos necesarios y definiendo los procedimientos y mecanismos para efectuar dichas actividades. Estas copias de seguridad deben programarse regularmente, para facilitar la recuperación y reconstrucción de datos y sistemas como estaban cuando se efectuaron las copias.

En situaciones donde se subcontraten servicios, la Universidad tiene la obligación de asegurar que los proveedores se adhieran a lo estipulado en esta política y revisar de manera periódica su cumplimiento.

Las copias de seguridad deben ser cifradas, especialmente aquellas que contienen información catalogada como Confidencial. Para este fin, se deben implementar los procedimientos y mecanismos establecidos por la dirección de tecnologías de la información.

La Dirección de Tecnología es responsable de definir y poner en práctica los procedimientos necesarios para la generación, restauración de almacenamiento y manejo de las copias de respaldo de información, garantizando su confidencialidad, integridad y disponibilidad en todo momento.

2.2 Protección contra software malicioso

La administración de herramientas de protección contra software malicioso es responsabilidad de la dirección de tecnologías de la información, para prevenir que, ya sean usuarios o atacantes, modifiquen los parámetros o desactiven sus módulos de protección sin autorización previa o por falta de restricción de privilegios. Asimismo, debe gestionar o configurar las herramientas de protección contra software malicioso para garantizar que la información y la plataforma tecnológica estén libres de malwares.

Se debe tener un catálogo de softwares autorizados para utilizar en los dispositivos de la organización, adecuados para las actividades de los trabajadores y proveedores de la Universidad. Además, es

Documento Controlado, prohibida su reproducción parcial o total sin autorización

responsabilidad de la Dirección de Tecnologías de la Información implementar medidas de control para prevenir o identificar el acceso a sitios web que son sospechosos de tener contenido malicioso. Asimismo, se encarga de hacer revisiones regulares a los sistemas de protección contra malware, para detectar cualquier alteración y disminuir la incidencia y difusión de software malicioso dentro de la organización. Cualquier detección de programa malicioso debe ser debidamente documentado siguiendo el procedimiento de Gestión de Incidentes.

El servicio de gestión de correos electrónicos que ha contratado Universidad Mayor ofrece garantías de revisión contra software malicioso y contra la recepción de correos no deseados (spam). Se prohíbe abrir archivos adjuntos de correos electrónicos provenientes de fuentes desconocidas, sospechosas o no confiables. Es imperativo informar sobre estas situaciones al Dirección de Tecnología para determinar conjuntamente el accionar.

Es necesario realizar revisiones periódicas o establecer sistemas de alerta automáticos para asegurar que todas las estaciones de trabajo cuenten con las herramientas de protección contra programas malignos instalados y actualizados. Si se detecta que esto no cumple, la situación debe ser notificada a las áreas correspondientes y manejarla como un incidente de seguridad.

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