Universidad Mayor | Dirección de Tecnologías de la Información

POLÍTICA USO DE CORREO ELECTRÓNICO INSTITUCIONAL

POLÍTICA USO DE CORREO ELECTRÓNICO INSTITUCIONAL[1]

I. OBJETO

La presente política establece las pautas para el uso responsable y eficiente del correo electrónico corporativo para todos los trabajadores de la Universidad Mayor. Esta política busca garantizar la seguridad, confidencialidad, integridad y eficacia de las comunicaciones electrónicas dentro de la organización.

Con esta Política, la Universidad Mayor, se compromete, a proteger sus activos de información, estableciendo una adecuada gestión del riesgo informático, asegurando el cumplimiento de los requisitos legales.

II. ALCANCE

Esta política se aplica a todos los trabajadores, contratistas, consultores y cualquier otra persona que utilice los recursos de correo electrónico corporativo de la Universidad Mayor. Se extiende a todos los dispositivos y redes de la empresa, ya sean propiedad de la empresa o personales, cuando se utilicen para asuntos relacionados con la empresa.

III. DECLARACIÓN INSTITUCIONAL

La Universidad Mayor reconoce el valor estratégico del correo electrónico corporativo como medio esencial para la comunicación académica, administrativa y de gestión institucional. En este sentido, declara su compromiso de fomentar un uso responsable, seguro y eficiente de esta herramienta, entendiendo que constituye un activo crítico para la protección de la información, la continuidad de los procesos y el cumplimiento normativo.

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

Con esta política, la Universidad se compromete a resguardar la confidencialidad, integridad y disponibilidad de las comunicaciones electrónicas, estableciendo directrices claras que permitan prevenir riesgos, garantizar el cumplimiento de la legislación vigente y promover buenas prácticas en la gestión de la información digital.

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.

V. DEFINICIONES

Para efectos de la presente Política se entenderá por:

Concepto	Descripción
Cultura Organizacional	Conjunto de valores, normas y comportamientos compartidos dentro de una organización.
Autenticación de dos factores (2FA):	Método de verificación que requiere dos formas distintas de identificación para acceder a una cuenta.
Enlaces maliciosos:	Vínculos incluidos en correos electrónicos o sitios web que llevan a páginas fraudulentas o peligrosas.

Cifrado:	Proceso de convertir información legible en un código ilegible de un mensaje o documento.
Ofuscación de correo electrónico:	Técnica para ocultar direcciones de correo electrónico de los bots de spam.

VI. ÁMBITOS DE ACCIÓN

1. Política de uso de correo electrónico

La utilización de la cuenta de correo electrónico empresarial debe restringirse a las actividades relacionadas con las funciones y responsabilidades del personal, según lo establecido en su contrato de trabajo o convenio de servicios.

1.1. Acerca del correo electrónico

La Dirección de Tecnologías de la Información de la Información será la única responsable de la operación y provisión del sistema de correo electrónico de la Universidad Mayor. Para lo anterior, se emplearán el dominio "@umayor.cl" y "@mayor.cl". Se procederá a la creación, bloqueo o eliminación de cuentas de correo electrónicos, sólo en el caso que sean visadas por la Dirección de Personas y/o Direcciones de áreas respectivas.

En casos excepcionales, se podrá definir cuentas de correo electrónico asociadas a sistemas, para fines indispensables y absolutamente técnicos. Se podrán crear listas de correo con el propósito de ser contacto corporativo asociada a equipo de personas responsables, las que deberán ser debidamente justificadas ante el director de tecnología de la información.

Se podrán eventualmente crear cuentas genéricas de correo o para grupos de usuarios, las que deberán ser debidamente justificadas ante el director de tecnología de la información. El personal no podrá contar con más de una cuenta de correo electrónico.

Se promoverá el correcto uso del correo electrónico corporativo, para lo cual, se debe garantizar capacitaciones regulares para los trabajadores sobre las políticas y procedimientos del uso del correo electrónico corporativo, abarcando aspectos como la seguridad de la información, la detección de correos electrónicos fraudulentos, y el manejo adecuado de la información confidencial.

1.2. Uso apropiado del correo corporativo

Los trabajadores de la Universidad Mayor deben familiarizarse con las directrices establecidas por la empresa respecto al uso del correo electrónico corporativo, lo que incluye las políticas y procedimientos de seguridad de la información, el uso aceptable y la retención de datos.

En relación con las contraseñas de correo electrónico corporativo, es fundamental utilizar contraseñas robustas, actualizarlas regularmente y abstenerse de compartirlas con otras personas.

Se debe evitar enviar información confidencial o sensible a través del correo electrónico corporativo, a menos que sea absolutamente necesario, y utilizar métodos seguros de cifrado para transmitir datos sensibles.

Asimismo, todo personal externo, contratista o asesor que preste servicio a la Universidad Mayor que por sus funciones requiera comunicación interna, intercambio de documentos, coordinación de proyectos, entre otros, podrá utilizar el correo electrónico corporativo. Sin embargo, estas excepciones deben ser claramente definidas y aprobadas por la Dirección de Tecnologías de la Información y la Dirección de Personas, cumpliendo con los requisitos mínimos de contar con una relación contractual con la Universidad Mayor, firmar un Acuerdo de Confidencialidad y contar con la autorización de la Dirección de Tecnologías de la Información para la creación de la cuenta corporativa.

1.3. Contraseña segura

Se debe evitar utilizar información personal como nombres, fechas de nacimiento o palabras comunes en las contraseñas, ya que esta información puede ser fácilmente adivinada por los atacantes.

Las contraseñas, deben contar con las características detalladas en la política de control de acceso.

La Dirección de Tecnologías de la Información debe programar los cambios de las contraseñas regularmente, al menos cada tres meses, para reducir el riesgo de que sean comprometidas por ataques de fuerza bruta o filtraciones de datos, además se debe bloquear el acceso después del quinto intento de ingreso fallido.

1.4. Identificación del remitente

Los trabajadores de la Universidad Mayor deben examinar cuidadosamente la dirección de correo electrónico del remitente para detectar posibles errores ortográficos o variaciones que puedan indicar un intento de suplantación de identidad. Deben desconfiar de correos electrónicos no solicitados, especialmente si contienen enlaces o solicitudes de información confidencial.

El servicio de correo electrónico, controlado por la Dirección de Tecnologías de la Información, deberá contar, al menos, con las configuraciones adecuadas, de las siguientes características de seguridad, como DMARC (Domain-based Message Authentification Reporting and Conformance), DKIM (DomainKeys Identified Mail) o SPF (Sender Policy Framework) para verificar la autenticidad del remitente.

Antes de responder a un correo electrónico o seguir cualquier instrucción proporcionada en él, se debe tomar el tiempo necesario para investigar la autenticidad del remitente y la legitimidad del correo electrónico.

1.5. Correos sospechosos

Ante el recibo de correos sospechosos, los trabajadores de la Universidad Mayor deben verificar la dirección de correo electrónico del remitente para asegurarse de que sea legítima y corresponda a una fuente confiable.

Además, deben evitar hacer clic en enlaces, incluidos en correos electrónicos sospechosos, especialmente si provienen de remitentes desconocidos o no solicitados. En su lugar, se recomienda visitar el sitio web directamente escribiendo la URL en el navegador. No deben proporcionar información personal, financiera o de inicio de sesión en respuesta a correos electrónicos sospechosos, incluso si parecen provenir de una fuente legítima.

La Dirección de Tecnologías de la Información, deberá incorporar en el sistema de correo electrónico, herramientas para el control de antimalware y antispam para escanear y filtrar correos electrónicos sospechosos y de manera general se podrán implementar alguno de estos criterios para su control:

- Controles SPF / DKIM / DMARC
- Control DNSSEC
- Listas de reputación de IP’s.

Los trabajadores de la Universidad Mayor deben mantenerse al tanto de las estafas y técnicas de phishing más recientes y compartir esta información con los demás trabajadores para ayudar a protegerlos contra posibles amenazas. Ante cualquier identificación de un posible ataque de seguridad, se debe tomar los resguardos e informar el incidente a través de los canales oficiales definidos en la política de gestión de incidentes de la información.

1.6. Utilizar la copia oculta (BCC o CCO)

Los trabajadores de la Universidad Mayor deben utilizar la copia oculta sólo cuando sea necesario proteger la privacidad de los destinatarios. Además, deben evitar enviar correos electrónicos a un gran número de destinatarios en la copia oculta, ya que esto puede dificultar la gestión y seguimiento del correo electrónico. En su lugar, se debe considerar utilizar herramientas de correo electrónico masivos o grupos de correo para gestionar listas de destinatarios grandes.

1.7. Análisis de adjuntos

Los trabajadores de la Universidad Mayor deben verificar el tipo de archivo y evaluar si es apropiado para el contexto del correo electrónico. Se debe ser especialmente cauteloso con los archivos ejecutables (.exe) y los archivos comprimidos (.rar; .zip) ya que podrían potencialmente contener un malware.

Se recomienda verificar el remitente del correo electrónico y la coherencia con los contactos conocidos. Si se recibe un archivo adjunto de una fuente desconocida o inesperada, se debe proceder con precaución y considerar no abrirlo hasta confirmar su autenticidad.

La Dirección de Tecnologías de la Información debe mantener el software antivirus actualizado para escanear todos los archivos adjuntos antes de abrirlos. Se debe asegurar que el software antivirus esté configurado para analizar en tiempo real y escanear todos los tipos de archivos buscando amenazas.

Si el archivo adjunto está firmado digitalmente, se debe verificar la firma para asegurarse de que proviene de una fuente confiable y no ha sido modificado desde su creación. Se recomienda utilizar herramientas de verificación de firma digital para realizar esta tarea.

1.8. Inspección de enlaces

Los trabajadores de la Universidad Mayor deben evitar hacer clic en enlaces incluidos en correos electrónicos no solicitados o mensajes de remitentes desconocidos. Comúnmente son utilizados en ataques de phishing.

Antes de hacer clic en un enlace, se debe verificar su autenticidad mediante la inspección de la URL y la confirmación del dominio. No se debe confiar en enlaces acortados ni enlaces con errores obvios.

La Dirección de Tecnologías de la Información debe emplear herramientas de seguridad cibernética, como filtros de correo electrónico, software antivirus y soluciones de seguridad de red, para detectar y bloquear enlaces maliciosos antes de que lleguen a la bandeja de entrada.

Los trabajadores de la Universidad Mayor deben priorizar los enlaces que utilizan el protocolo HTTPS en lugar de HTTP. Antes de hacer clic en un enlace, se recomienda a los trabajadores de La Universidad Mayor pasar el cursor sobre el (sin hacer clic) para ver la URL del destino completa. Esto revelará la dirección real del enlace y te permitirá evaluar su seguridad antes de tomar una decisión.

Algunos enlaces pueden contener contenido oculto o redirecciones que no son evidentes a simple vista. Se recomienda utilizar herramientas de análisis de enlaces para descubrir cualquier redireccionamiento no deseado o contenido malicioso.

Si los trabajadores sospechan de la autenticidad de un enlace, se debe reportar a la Dirección de Tecnologías de la Información para su análisis y posible bloqueo. Los trabajadores no deben acceder al enlace si no están seguros de su procedencia.

1.9. Envío de correos electrónicos

El servicio de correo no cifra la información contenida en los correos, pudiendo ser eventualmente accesibles por terceros. De requerirse niveles adicionales de protección, se recomienda utilizar técnicas de cifrado o métodos seguros de transmisión.

1.10. Desactivar el formato HTML

La Dirección de Tecnologías de la Información debe configurar el cliente de correo electrónico para desactivar la visualización de correos electrónicos en formato HTML y configurarlo para mostrar solo texto plano.

No obstante, aunque esto puede mejorar la seguridad, los trabajadores de la Universidad Mayor deben verificar los correos electrónicos sospechosos, especialmente aquellos que solicitan información personal o financiera.

La Dirección de Tecnologías de la Información debe asegurarse de mantener actualizado el cliente de correo electrónico y cualquier software relacionado para beneficiarse de las últimas mejoras de seguridad.

Además, debe proporcionar orientación a los trabajadores de la Universidad Mayor sobre los riesgos de seguridad asociados con los correos electrónicos en formato HTML y cómo desactivar este formato en su cliente de correo electrónico si lo desean.

Como seguridad adicional, algunas extensiones de seguridad para clientes de correo electrónico pueden ayudar a bloquear el contenido HTML malicioso o proporcionar funciones adicionales de seguridad y privacidad.

1.11. Cifrado y firma digital

La Dirección de Tecnologías de la Información debe emplear protocolos de cifrados seguros, como SSL/TLS para la transmisión de datos a través de internet y PGP/GPG para la comunicación segura por correo electrónico.

Al utilizar sitios web seguros, se debe verificar que los certificados SSL/TLS sean válidos y confiables para asegurarse que la conexión esté protegida mediante cifrado.

1.12. Método de Ofuscación de correo electrónico

Se recomienda evitar publicar las direcciones de correo corporativas en páginas web ni en redes sociales sin utilizar técnicas de ofuscación. Si no, esas cuentas pueden captarlas para incluirlas en listas de envío de spam.

1.13. Evitar las redes públicas

Los trabajadores de la Universidad Mayor deben preferir el uso de redes privadas y seguras, que ofrecen cifrado de datos y protección contra amenazas cibernéticas.

Los trabajadores de la Universidad Mayor deben evitar realizar transacciones financieras o enviar información confidencial, mientras estén conectados a una red Wifi pública. De ser necesario, debe utilizar la VPN de la compañía para proteger la transmisión de datos.

La Dirección de Tecnologías de la Información debe desactivar la configuración de conexión automática a redes Wifi-públicas en los activos para evitar conectarse inadvertidamente a redes no seguras.

1.14. Referencia normativa al Decreto Universitario N°16-2020

En todo lo no contemplado expresamente en la presente política, serán aplicables las disposiciones establecidas en el Decreto Universitario N°16 de 2020, o el instrumento que lo reemplace, que aprueba los

Instructivos de seguridad relativos al uso de correos electrónicos institucionales y de servicios de internet en la Universidad Mayor.

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