POLÍTICA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

UNIVERSIDAD MAYOR
para espíritus emprendedores

Contenido

Política aprobada mediante Decreto N° 44 de 17 de octubre de 2023.

1 Introducción

La Universidad Mayor, en adelante también como la "Universidad", tiene como misión la formación de personas a través de una experiencia educativa que estimule en ellas un comportamiento ético, una actitud de emprendimiento, innovación, liderazgo y respeto por la diversidad cultural y social. Para ello, imparte programas de pregrado y postgrado de excelencia y realiza actividades de generación, articulación y difusión del conocimiento que contribuyan a la comunidad nacional en los ámbitos cultural, educativo, social y económico, considerando el contexto de un mundo global y las normas del rigor científico, para cumplir este fin, la Universidad reconoce que los activos de información son esenciales y que como tales se requiere su protección para garantizar la continuidad operativa, asegurando la confidencialidad, disponibilidad y la integridad de la información.

La Universidad ha definido como indispensable adoptar las medidas organizativas y técnicas necesarias para garantizar el pleno funcionamiento de los activos tecnológicos a fin de protegerlos frente a cualquier daño, sea accidental o provocado, que puedan afectar a la disponibilidad de los activos, la integridad de la información, su confidencialidad y la correcta autenticación de los usuarios, de forma de estar protegidos contra amenazas de rápida evolución que puedan vulnerar el valor y/o la calidad de la información y la continua prestación de servicios por parte de la Universidad.

Dentro de ese contexto, el propósito de la presente Política de Gestión de la Seguridad de la Información de la Universidad, en adelante, la Política, es establecer las bases de funcionamiento y operación de sus activos tecnológicos de forma de asegurar su efectiva prestación de servicios y el cuidado de la información, de forma de evitar interrupciones en su flujo de funcionamiento, modificaciones indebidas y fugas de información o conocimiento hacia personas y entidades no autorizadas.

2 Objetivo

2.1 Objetivo General

Establecer los principios y marco general de trabajo de la Universidad Mayor para administrar, mantener, sensibilizar, monitorear y revisar el Sistema de Gestión de Seguridad de la Información (SGSI) acorde a las definiciones estratégicas, la misión/visión y objetivos estratégicos, asegurando la confidencialidad, integridad y disponibilidad de los activos de información a través de su adecuada implementación, asignación de roles, funciones y responsabilidades.

2.2 Objetivos específicos

a) Asegurar el cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que estén orientados hacia la seguridad de la información.
b) Establecer los niveles de acceso apropiados a la información, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema, proceso, actividad crítica y usuario.
c) Implementar una metodología enfocada en la gestión de riesgo institucional y establecer un marco de gestión de riesgo cibernético para cada sistema, proceso, actividad crítica, que permita alcanzar los objetivos estratégicos.
d) Apoyar al modelo de gestión de continuidad del negocio.
e) Definición del ámbito de trabajo y responsabilidades corporativas e individuales respecto al uso de los recursos tecnológicos que provee la Universidad y al manejo de la información.
f) Establecer mecanismos de auditoría y control de los activos de información y tecnologías de procesamiento.
g) Comunicar, concientizar, capacitar, sensibilizar e informar sobre los lineamientos de seguridad de la información a toda la Universidad.

3 Alcance

La presente política está dirigida a todos los que tenga parte y legítimo acceso a los sistemas de información de la Universidad. Aplica a toda la comunidad universitaria, a sus autoridades, directivos, funcionarios, independientemente se encuentren en modalidad presencial o teletrabajo, estudiantes, docentes (planta u honorarios). Indistintamente del campus o ubicación geográfica específica que se trate. También considera a todos los prestadores de servicios y colaboradores de empresas contratistas y subcontratistas.

4 Roles y Responsabilidades

- **Comité de Ciberseguridad:**

El Comité de Seguridad de la Información, en adelante, el Comité, tiene por rol velar por la efectiva vigencia de la Política de Gestión de la Seguridad de la Información en la Universidad, así como de los instructivos y documentos que se deriven de la presente Política.

Está compuesta por las siguientes personas:

1. Contralor/a (quien lo preside).
2. Secretario/a General, o quien le represente.
3. Vicerrector/a de Asuntos Globales y Desarrollo, o quien le represente.
4. Oficial de Seguridad de la Información (CISO).
5. Oficial de Protección de Datos (DPO).
6. Director/a de Personas, o quien le represente.
7. Director/a de Comunicación Estratégicas, o quien le represente.
8. Director/a de Ciberseguridad, o quien le represente.
9. Director/a de Tecnologías de la Información, o quien le represente.
10. Director/a de la Unidad de Auditoría Interna.
11. Dirección de Control de Procesos y Gestión de Riesgos.

El Comité se reunirá a instancias del/la Contralor/a con una periodicidad trimestral, salvo que la adopción de medidas urgentes aconseje otra medida distinta, y podrá invitar a sus reuniones a las personas que

considere oportunas en función de los temas a tratar; el quorum para sesionar será el de la mayoría de sus miembros.

En materia de seguridad, el Comité tendrá las siguientes funciones:

a. Informar regularmente del estado de la seguridad de la información al Rector de la Universidad.
b. Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
c. Elaborar la estrategia de evolución de la Universidad en lo que respecta a la seguridad de la información.
d. Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, evitando duplicidades.
e. Revisar regularmente la Política de Gestión de la Seguridad de la Información y realizar propuestas de mejora, y someterlas al Directorio de la Universidad para su aprobación.
f. Aprobar políticas específicas, procedimientos e instrucciones en desarrollo de lo dispuesto en la Política de Gestión de la Seguridad de la Información de la Universidad.
g. Recomendar requisitos de formación y calificación de administradores, operadores y usuarios de los activos tecnológicos de la Universidad, desde el punto de vista de la seguridad de la información.
h. Monitorear el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de dicha gestión.
i. Velar por la coordinación de las diferentes áreas de la Universidad en la gestión de incidentes de seguridad de la información.
j. Aprobar planes de mejora de la seguridad de la información de la Universidad.
k. Priorizar las actuaciones en materia de seguridad de la información cuando los recursos sean limitados.
l. Velar por que la seguridad de la información sea considerada en todos los proyectos de la Universidad, desde su planteamiento inicial hasta su puesta en operación.
m. Resolver los conflictos de responsabilidad que puedan aparecer entre los responsables de diferentes áreas, elevando al órgano competente aquellos casos en los que no tenga suficiente autoridad para decidir.
n. Velar por el efectivo respeto del derecho a la protección de datos personales en las operaciones de tratamiento de datos que lleve adelante la Universidad.

- **Dirección de Ciberseguridad:**

La dirección tendrá a su cargo el Centro de Operaciones de Seguridad (SOC), unidad responsable de detectar e identificar riesgos y amenazas, actuales y potenciales, que puedan poner en riesgo o dañar los activos tecnológicos de la Universidad, así como implementar medidas de reacción, a requerimiento del Oficial de Seguridad de la Información y en coordinación con la Dirección de Tecnologías de la Información.

La dirección establece el Equipos de Respuesta frente a Incidencias de Seguridad Informática (CSIRT) para evaluar y responder a los incidentes de seguridad de la información y aprender de estos, y proporcionar la coordinación, gestión, retroalimentación y comunicación necesaria.

De igual forma, esta Dirección tendrá las siguientes funciones:

a. Gestionar la formulación y ejecución del plan estratégico de Ciberseguridad, en línea con los objetivos del negocio y conforme al marco normativo, legal y regulatorio.
b. Asegurar el cumplimiento de la estrategia de Ciberseguridad definida por la organización, así como de las políticas, normas y procedimientos en este ámbito.
c. Desarrollar la cultura de Ciberseguridad y entregar los conocimientos que permitan identificar ciberamenazas que pongan en riesgo la información y los activos de información de la Universidad.
d. Detectar las amenazas y vulnerabilidades para prevenir los incidentes de Ciberseguridad de manera oportuna, con el objetivo de proteger la infraestructura, los servicios y operaciones de la Universidad.
e. Maximizar el uso de las tecnologías de protección existentes e incorporar nueva.
f. Proteger los datos y activos de información de la Universidad de las ciberamenazas existentes, bajo los lineamientos del Oficial de Seguridad y los resultados de los análisis de riesgos.
g. Adquirir y analizar información para identificar, rastrear, predecir y contrarrestar intenciones y actividades de ciberatacantes.
h. Administrar y monitorear el correcto funcionamiento de las herramientas tecnológicas de seguridad implantadas en ambientes de tecnológicos.
i. Controlar, administrar y monitorear los accesos y privilegios de usuarios.

- **Dirección de Gobierno de Datos y Analítica:**

Esta unidad será responsable de la seguridad en el tratamiento de datos de carácter personal y datos sensibles, en todo su ciclo de vida (recogida de los datos, conservación y utilización de los datos, comunicación de los datos) y de establecer las políticas de gobernanza de datos, se rige bajo las recomendaciones y buenas prácticas de la normativa internacional y cumplimiento de la legislación chilena Ley N° 19.628 Sobre Protección de la Vida Privada. Es la responsable de la gestión de riesgos, relacionada a la protección de la vida privada, e implementación de controles para salvaguardar la integridad de los datos de carácter personal.

El rol de Oficial de Protección de Datos (DPO), recaerá sobre quién ostente el cargo de Director de Gobierno de Datos y Analítica.

- **Oficial de Seguridad de la Información:**

El Oficial de Seguridad de la Información (CISO) es el responsable máximo en planificar, desarrollar, controlar y gestionar las políticas, procedimientos, instructivos y planes de acción con el fin de implementar una efectiva seguridad de la información en la Universidad, teniendo especialmente a su cargo las decisiones sobre el cumplimiento regulatorio por parte de la misma, la continuidad del negocio en lo que a activos tecnológicos se refiere, y es el responsable último por las decisiones de seguridad corporativa.

De igual forma, son roles del Oficial de Seguridad de la Información:

a. Tendrá la responsabilidad de coordinar las actividades relacionadas a la gestión de la Política de Seguridad de la Información en la Universidad.
b. Coordinar las actividades del Comité de Ciberseguridad.
c. Coordinar las debida respuesta y priorización al tratamiento de incidentes y riesgos vinculados a los activos de información.

d. Mantener la coordinación con las unidades internas y con entidades externas para apoyar los objetivos de la seguridad de la información.
e. Mantener la aplicabilidad de este documento acorde a las prácticas operacionales de la Universidad, por lo que es responsable de generar las modificaciones necesarias para que éste siempre actualizado. Junto con lo anterior, es responsable de gestionar la publicación y dar a conocer las diferentes políticas que derivan de la Política de Seguridad de la Información.

El rol de Oficial de Seguridad de la Información, CISO, recaerá sobre quién ostente el cargo de Director de Ciberseguridad de la Universidad.

Para el desarrollo de sus labores cuenta con la debida colaboración de la Dirección de Tecnologías de la Información, Dirección de Ciberseguridad y cuando sea necesario con el Centro de Investigación en Ciberseguridad (CICS) de la Universidad.

- **Dirección de Tecnologías de la Información:**

Esta dirección tendrá a su cargo el Centro de Operaciones de Red (NOC) encargada de la seguridad operativa, implementar y gestionar las herramientas tecnológicas relacionada a la seguridad de la información. Gestiona y soluciona los incidentes de seguridad de la información tecnológicos detectados y normaliza los servicios para la operación cotidiana de la Universidad.

- **Unidad de Auditoría de Seguridad de la Información:**

La unidad de auditoría tendrá dependencia directa de la Contraloría Institucional y por medio de estas se comunicarán los informes de auditoría a la alta dirección y partes interesadas.

Será responsable de llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el Sistema de Gestión de la Seguridad de la Información, su implementación, esta mantenida de manera eficaz y si se cumplen los requisitos propios de la Universidad para su SGSI.

La Universidad planificará, establecerá, implementará y mantendrá un programa de auditoría anual, estos programas de auditoría deberán tener en cuenta la importancia de los procesos críticos de la Universidad.

5 Documentos relacionados

- Norma Internacional ISO 27001 “Sistema de Gestión de Seguridad de la Información”.
- Ley N° 19.628 Sobre la Protección de la Vida Privada.
- Ley N° 21.459 Establece Normas Sobre Delitos Informáticos.
- Ley N° 17.336 de Propiedad Intelectual.
- Ley N° 19.799 Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Ley N° 19.496, Establece normas sobre protección de los derechos de los consumidores.

6 Ámbito de la Seguridad de la Información

La Universidad a través del Comité de Ciberseguridad y la Dirección de Ciberseguridad se compromete a establecer, implementar, mantener y mejorar de manera continua el Sistema de Gestión de la Seguridad de la Información, basado en la norma internacional ISO 27001.

El SGSI ofrece a la Universidad la capacidad de proteger, preservar y administrar, la confidencialidad, integridad y disponibilidad de la información institucional, salvaguardando la precisión de esta a través de:

a) Servicios de redes, contenidos y aplicaciones soportadas en las plataformas apropiadas protegiendo los mecanismos de tratamiento, almacenamiento y comunicación.
b) Personal competente y comprometido con una cultura de seguridad reflejada en la aceptación y aplicación de las directrices establecidas.
c) El cumplimiento de las disposiciones legales y regulatorias emitidas por los diferentes organismos.

Para estos efectos, se llevará a cabo un proceso de análisis de riesgos y, de acuerdo con su resultado, se implementarán acciones de mitigación, con el fin de tratar aquellos que sean considerados críticos para el servicio de acuerdo al alcance definido del SGSI.

Por lo anterior la Universidad identificará, valorará, tratará y monitoreará los riesgos asociados con la operación de sus tareas, y de sus activos de la información, asegurando el eficiente cumplimiento de las

funciones sustantivas de la entidad apoyada en una adecuada gestión de dichos riesgos, mediante la aplicación de los controles consignados en el Anexo A de la ISO 27001.

La Universidad además implementará las medidas de sensibilización para la formación y toma de conciencia de los funcionarios y partes interesadas en todos los aspectos relacionados con la seguridad de la información y del SGSI. A su vez, cuando los funcionarios y/o las partes interesadas incumplan la presente política de seguridad de la información o con las políticas derivadas de ella.

7 Vigencia, Actualización y Evaluación de la Política

La política se considerará vigente desde su fecha de aprobación por parte de la autoridad. La presente política será revisada y actualizada según corresponda anualmente, o cuando la Universidad lo requiera, para asegurar su continuidad e idoneidad considerando cambios externos o internos que puedan afectarla.

La política será aprobada por el Comité de Ciberseguridad y la Dirección de Ciberseguridad promoverá la revisión permanente de esta política, generando propuestas de actualización con el objetivo de apoyar el ciclo de mejora continua del SGSI. El Comité de Ciberseguridad asignará la responsabilidad de ejecutar una revisión de cumplimiento de la presente política por medio de auditorías internas, cuando se estime necesario, también control documental requeridos para el funcionamiento del SGSI.

8 Difusión

El mecanismo de difusión de la presente política será a través de la Intranet, circulares informativas, correos electrónicos masivos o cualquier otro medio que el Comité de Ciberseguridad estime pertinente, procurando apoyar la concientización con infografías que faciliten la comprensión de esta política para toda la Universidad.

En caso de modificación de cargo y/o funciones, o para los nuevos funcionarios y prestadores se debe realizar formación sobre Seguridad de la Información y conocimiento de la presente política.

La presente política estará disponible para todas las partes interesadas definidos en el apartado 3).

9 Sanciones aplicables

El incumplimiento de la presente política conllevará la aplicación de las medidas disciplinarias contempladas en el Reglamento Interno de Orden, Higiene y Seguridad de la Universidad Mayor, o el término de la relación laboral por incumplimiento grave a las obligaciones que impone el contrato de trabajo; o el término anticipado del respectivo contrato de prestación de servicios a honorarios u otras sanciones, según sea el caso.

10 Definiciones o Glosario de Términos

a) **Datos de carácter personal:** Es lo relativo a cualquier información concerniente a personas naturales, identificadas o identificables. El tratamiento de estos datos sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello.
b) **Datos sensibles:** Aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.
c) **Seguridad de la Información:** preservación de la confidencialidad, integridad y la disponibilidad de la información.
d) **Disponibilidad:** propiedad de ser accesible y estar listo para su uso a demanda de la Universidad.
e) **Confidencialidad:** propiedad de la información por la que mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.
f) **Integridad:** propiedad de exactitud y completitud.
g) **Control:** medida que modifica un riesgo.
h) **Sistema de Información:** aplicaciones, servicios, activos de tecnologías de la información y otros componentes para manejar información.
i) **Amenaza:** causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a la Universidad como institución.

j) Vulnerabilidad: debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

k) Incidente: uno o múltiples eventos de seguridad de la información relacionados e identificados que puede(n) dañar los activos de la Universidad o comprometer sus operaciones.

l) Activos de información: Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la Universidad, cualquiera sea el formato que la contenga, equipos y sistemas que la soporten. Por ejemplo: dispositivos móviles, tarjetas de accesos, software, equipamiento computacional, personal, edificios, infraestructura tecnológica y física (CSIRT GOB).

11 Control de cambios

Control de cambios						
Versión	**Fecha Aprobación/Vigencia**	**Numeral (N° del título modificado)**	**Motivo del Cambio**	**Descripción del Cambio**	**Revisado por**	**Aprobado por**
1	17/12/2020	No aplica	Creación	Primera versión de la Política (Decreto Nº 15)	Dirección de Ciberseguridad	Comité de Ciberseguridad
2	01/09/2023	Todos	Actualización	Segunda versión de la Política	Dirección de Ciberseguridad	Comité de Ciberseguridad