RESOLUCIÓN DE RECTORÍA N°108/2025

MAT.: Aprueba Política de Ciberseguridad.

Viña del Mar, 05 de septiembre de 2025.

VISTOS:

1. Lo establecido en los Estatutos de la Universidad.
2. Las facultades que confiere la normativa universitaria, específicamente el Reglamento Orgánico de la Universidad Viña del Mar.

CONSIDERANDO:

1. Que la Universidad cuenta con información académica, administrativa y personal contenida en diversos sistemas informáticos, la cual requiere medidas de seguridad adecuadas para prevenir accesos no autorizados, pérdida, alteración o uso indebido.
2. Que, dada la naturaleza y criticidad de las funciones universitarias —docencia, investigación, vinculación con el medio y gestión institucional—, resulta esencial garantizar la **disponibilidad, integridad, confidencialidad y trazabilidad** de los sistemas y servicios de información.
3. Que es necesario establecer lineamientos institucionales que permitan **proteger los datos personales e institucionales**, **asegurar la continuidad académica y operativa**, **prevenir incidentes de ciberseguridad**, y **fortalecer las capacidades y la cultura digital** de la comunidad universitaria, mediante la formación y la adopción de buenas prácticas.
4. La propuesta de la Dirección de Tecnologías de la Información.
5. La opinión favorable de la Vicerrectoría de Finanzas.
6. La opinión favorable del Comité de Rectoría.
7. El acuerdo del Directorio en sesión del 19 de agosto de 2025.

RESUELVO:

1. **DICTAR** la Política de Ciberseguridad de la Universidad Viña del Mar.
2. **FIJAR** el texto de la Política de Ciberseguridad de acuerdo con documento que se adjunta y que forma parte integrante de la presente resolución.

Comuníquese, publíquese y archívese.

UVM
UNIVERSIDAD VIÑA DEL MAR
RECTORÍA

CARLOS ISAAC PÁLYI
Rector

CIP/MIC/ppr.
Distribución:
Comunidad Universitaria.
c.c.: Archivo.

UVM

UNIVERSIDAD VIÑA DEL MAR

POLÍTICA DE CIBERSEGURIDAD

POLÍTICA DE CIBERSEGURIDAD

DEFINICIÓN DE CIBERSEGURIDAD

En la Universidad Viña del Mar, la Ciberseguridad y Seguridad de la Información Digital comprenden el conjunto de medidas, normativas y procedimientos diseñados para proteger la información y los servicios digitales institucionales contra ciberataques, accesos no autorizados, alteraciones, destrucción o pérdida, asegurando su confidencialidad, integridad y disponibilidad en todo momento.

OBJETIVO GENERAL

Garantizar la protección integral de los activos digitales, infraestructuras tecnológicas y servicios críticos de la Universidad, estableciendo procedimientos claros y efectivos que prevengan incidentes de ciberseguridad, mitiguen los riesgos y aseguren la continuidad operativa de la institución.

OBJETIVOS ESPECÍFICOS

Proteger la Información Institucional: Implementar medidas de seguridad que aseguren la confidencialidad, integridad y disponibilidad de la información de la institución.

Prevenir y Gestionar Riesgos: Identificar y evaluar los riesgos cibernéticos asociados con el manejo de la información y los activos digitales, estableciendo planes de mitigación efectivos para reducir su impacto.

Cumplimiento de Normativas: Asegurar el cumplimiento de leyes y estándares aplicables de ciberseguridad y protección de datos.

Concientización: Concientizar a los directivos, académicos y colaboradores de la Universidad Viña del Mar con el fin de fomentar buenas prácticas digitales.

FUNDAMENTO Y PROPÓSITO

Esta política se enmarca en el compromiso institucional de proteger los activos de información, los sistemas tecnológicos y las redes, y se alinea con las normativas nacionales e internacionales en materia de seguridad cibernética y protección de datos. El propósito es establecer un marco normativo que defina las acciones y directrices para mitigar los riesgos asociados a la accesibilidad de la información, garantizando la confidencialidad, integridad y disponibilidad de los activos digitales, proporcionando una seguridad razonable de la protección de los datos de usuarios, tanto interno como externos a la institución.

Universidad Viña del Mar promueve una cultura organizacional de la ciberseguridad y seguridad de la información, concientizando a los usuarios respecto a la importancia y participación de cada usuario en la protección de la información.

ALCANCE

La Política de Ciberseguridad e Infraestructura Tecnológica Institucional de la Universidad Viña del Mar se aplica a todos los miembros de la institución, incluidos los directivos, académicos y colaboradores, y cualquier otra persona que tenga acceso a los sistemas, activos digitales, datos o infraestructura tecnológica de la institución. Además, se extiende a todas las tecnologías utilizadas, incluyendo redes, servidores, bases de datos, aplicaciones, dispositivos móviles, y cualquier otro medio que maneje información institucional.

ÁMBITOS DE ACCIÓN

Para efectos de esta política, se definen los siguientes ámbitos de acción, los cuales serán el foco de las estrategias y actividades de la ciberseguridad de la institución:

Seguridad Física: Proteger los activos de información mediante medidas de seguridad física en las instalaciones, control de acceso a salas de servidores y equipos críticos, monitoreo de áreas sensibles y protección frente a siniestros, que pueden prevenirse mediante medidas como detección temprana o control de riesgos, y frente a desastres, cuya ocurrencia no puede predecirse aun aplicando acciones preventivas.

Seguridad Lógica y Digital: Implementar controles y procedimientos que aseguren la protección de la información y de los activos digitales almacenados, procesados o transmitidos electrónicamente, tales como cifrado, autenticación segura de usuarios, uso de autenticación multifactor y protección contra software malicioso, en el marco de la ciberseguridad y resguardando el cumplimiento normativo vigente en materia de seguridad informática.

Gestión de Vulnerabilidades: Establecer procedimientos para la identificación, evaluación y corrección de vulnerabilidades en sistemas, redes y aplicaciones, incluyendo revisiones periódicas y la aplicación oportuna de medidas de mitigación.

Gestión de Incidentes de Seguridad: Definir procedimientos para identificar y corregir vulnerabilidades en sistemas y activos digitales, mediante revisiones periódicas y aplicación oportuna de medidas correctivas. Detalles en el “Manual de Procedimientos de Ciberseguridad e Infraestructura Tecnológica”.

RESPONSABILIDADES

El cumplimiento de esta política será supervisado por la Dirección de Tecnologías de la Información, en colaboración con las diferentes áreas institucionales. Cada miembro de la comunidad universitaria es responsable de cumplir con los procedimientos establecidos para garantizar la seguridad de los sistemas, redes, datos y servicios digitales en todos los niveles.

CONTROL Y MONITOREO

Se mantendrá un monitoreo continuo para asegurar el cumplimiento de esta política y evaluar la efectividad de los procedimientos establecidos en su manual. Asimismo, se promoverá la mejora continua mediante la revisión periódica y, de ser necesario, la actualización de las políticas y procedimientos vinculados a la ciberseguridad, garantizando así la eficacia de nuestras prácticas institucionales.