

**APRUEBA POLÍTICA GENERAL DE
SEGURIDAD DE LA INFORMACIÓN DE LA
UNIVERSIDAD DE SANTIAGO DE CHILE.**

SANTIAGO, 11/08/2025 - 4102

VISTOS: El Decreto con Fuerza de Ley 29 de 2023, del Ministerio de Educación, que fija el Estatuto Orgánico de la Universidad de Santiago de Chile, adecuado al Título II de la Ley 21.094, sobre Universidades Estatales; el Decreto con Fuerza de Ley 1-19653, de 2000, que fija el texto refundido, coordinado y sistematizado de la Ley 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; el Decreto con Fuerza de Ley 29, de 2004, del Ministerio de Hacienda, sobre Estatuto Administrativo; la Ley 19.880, que establece Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado; la Ley 21.094 sobre Universidades Estatales; la Ley 21.663 Marco de Ciberseguridad, la Ley 19.628 sobre Protección de la Vida Privada; la Ley 21.459 que Establece Normas sobre Delitos Informáticos y deroga la Ley 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest; la Ley 21.595 de Delitos Económicos; el Decreto Supremo 136, de 2022, del Ministerio de Educación sobre nombramiento del Rector de la Universidad de Santiago de Chile; las Resoluciones 36 de 2024 y 8 de 2025, ambas de Contraloría General de la República.

CONSIDERANDO:

a) Que, para la Universidad de Santiago de Chile los activos de la información poseen gran valor estratégico y patrimonial, entendiéndose que, la información es el objeto a proteger, mientras que los activos de información son los elementos que permiten su uso, almacenamiento o transmisión. Por tanto, proteger los activos es una condición para resguardar adecuadamente la información.

b) Que, en ese sentido, resulta de suma importancia mantener la confidencialidad, integridad y disponibilidad de los activos de información protegiéndolos de una amplia gama de amenazas, con el fin de asegurar la continuidad de los procesos y minimizar o eliminar el daño que se les pudiera producir a éstos.

c) Que, de igual forma, existe la necesidad institucional de establecer un nuevo marco normativo interno estandarizado para la gestión, protección, aseguramiento de la calidad y uso de los datos institucionales, en concordancia con las modificaciones legales sobre la materia, como, por ejemplo, las leyes sobre Protección de la Vida Privada, la nueva ley de Delitos Económicos, la nueva ley marco de Ciberseguridad, entre otras.

d) Que, para la correcta observancia de lo precedentemente aludido, resulta necesario contar con un instrumento que establezca directrices y defina los criterios esenciales para las acciones y normativas relacionadas con la Seguridad de la Información.

e) Que, por su parte, mediante la Resolución Exenta N° 9968 de 2023, que modifica Resolución N° 1 de 2023, que fija la estructura orgánica de la Universidad de Santiago de Chile, se creó la Dirección Estratégica Informática, cuyo objetivo es garantizar la alineación efectiva entre las tecnologías de la información y la Corporación, asegurando que la tecnología sea un habilitador clave para el éxito institucional una ventaja competitiva.

RESUELVO:

1. APRUÉBASE la Política General de Seguridad de la Información de la Universidad de Santiago de Chile, cuyo texto es el siguiente:

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE SANTIAGO DE CHILE

I. DISPOSICIONES GENERALES

Artículo 1°: Declaración institucional: La Universidad de Santiago de Chile, en adelante indistintamente la “Universidad”, reconoce que la información y los activos de información son recursos críticos y de valor estratégico, por tanto, deben ser protegidos.

La Seguridad de la Información consiste en un conjunto de prácticas, métodos y normativas necesarias para mantener la confidencialidad, integridad y disponibilidad de la Información, a través de la identificación de riesgos y estrategias de prevención y de mitigación, tal como lo reconoce la norma ISO-27001.

La Universidad realizará los esfuerzos institucionales necesarios para desarrollar una cultura y gestionar la Seguridad de la Información y en particular de la Ciberseguridad de manera correcta y oportuna en base a la elaboración de políticas, normativas y procedimientos específicos para:

1. Controlar y proteger los activos digitales en cumplimiento de la normativa vigente.
2. Asegurar la continuidad operacional de los procesos de la universidad.
3. Apoyar la creación de una cultura de la ciberseguridad en la comunidad universitaria, mediante campañas de concienciación y otras acciones destinadas al efecto.

Esta Política tiene como objetivo entregar directrices generales en materias de ciberseguridad, en consonancia con lo establecido en la Ley N°19.628 sobre Protección de la Vida Privada, Ley N°21.459 que Establece Normas sobre Delitos Informáticos y deroga la

Ley N°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest, la ley N°21.595 de delitos económicos y la Ley N°21.663 sobre Ciberseguridad.

Adoptar medidas tendientes a promover la Seguridad de la Información la cual es responsabilidad de todos los miembros de la Comunidad Universitaria, independientemente de su nivel jerárquico y de su calidad jurídica, por lo que el uso normado e instruido de la información corporativa es una obligación.

II. ÁMBITO DE APLICACIÓN

Artículo 2°: Esta política aplica a todos los integrantes de la Comunidad Universitaria, como a los externos, sean personas naturales o jurídicas, que tengan acceso a la información corporativa, procesos y/o sistemas informáticos de que se dispone, para la ejecución de sus actividades institucionales.

En consecuencia, la presente política se aplica a todas las personas que hagan uso de los recursos y sistemas informáticos y de comunicaciones de la Universidad de Santiago de Chile, considerando la normativa vigente en el ámbito de seguridad de la información y ciberseguridad.

III. DIRECTRICES

Artículo 3°: En concordancia con esta política se generarán normativas internas específicas que permitan proteger los activos de información.

Artículo 4°: La información y los activos de información deben ser identificados, clasificados y protegidos según el grado de sensibilidad que les corresponda y su valor propio, sin hacer exclusiones de formato de presentación, con el objeto que esta no quede expuesta a personas y/o entidades externas, salvo en las situaciones y formas expresamente reguladas en la normativa vigente.

Artículo 5°: Los riesgos que impacten sobre la Seguridad de la Información deben ser considerados en todos los procesos de toma de decisiones.

Artículo 6°: Todos los miembros de la Comunidad Universitaria, como personas externas, sólo podrán acceder a la información y/o recursos que le sean debidamente autorizados, debiendo comunicar cualquier actividad o situación que afecte o pudiese afectar la seguridad de los activos de Información y/o recursos computacionales, informáticos o telemáticos.

Artículo 7°: Los planes anuales de capacitación de directivos/as y funcionarios/as deberán incluir actividades de concienciación y entrenamiento en materias de Seguridad de la Información, las que deben ser consideradas tareas prioritarias.

Artículo 8°: Esta política de seguridad de la información adhiere a todas las instrucciones emitidas por las siguientes instituciones, haciéndolas propias en lo pertinente, ANCI (Agencia Nacional de Ciberseguridad), ANPD (Agencia Nacional de Protección de Datos) y CMF (Comisión para el Mercado Financiero).

Artículo 9º: El incumplimiento de las políticas y normativas de Seguridad de la Información institucional constituirán incumplimiento de la normativa interna universitaria y dará lugar a los procedimientos disciplinarios que permitan esclarecer los hechos y responsabilidades asociadas a los mismos.

Todas las unidades académicas y administrativas de la Universidad serán responsables de la implementación y aplicación de las medidas y acciones de Seguridad de la Información que se definan, contando para ello con el apoyo de la Dirección Estratégica Informática.

IV. ROLES Y RESPONSABILIDADES

Artículo 10º: Con el objeto de materializar esta política se conformarán las siguientes instancias institucionales:

1. Oficial de Seguridad de la Información y Ciberseguridad (CISO): Es el/la funcionario/a al que se le asigna el rol responsable de la gestión de la Seguridad de la Información institucional, por lo tanto, serán sus funciones:

- Proponer y elaborar políticas de seguridad, diseñar controles y velar por su correcta implementación.
- Coordinar la respuesta ante incidentes de seguridad vinculados con activos de información.
- Identificar riesgos de Seguridad de la Información y proponer acciones de mitigación.
- Coordinar su labor con otras organizaciones a fin de mantenerse actualizado en materia de normativas o estándares aplicables a la Seguridad de la Información.
- Brindar asesoría institucional en materia de Seguridad de la Información, normativas y planes para el tratamiento de riesgos.
- Coordinar las sesiones del Comité de Seguridad de la Información de manera regular o cuando se observe un riesgo de alto impacto para la Universidad.

El Oficial de Seguridad de la Información y Ciberseguridad será nombrado por el/la Rector/a a propuesta del/la Director/a de la Dirección Estratégica Informática, por el período de tres (3) años, pudiendo ser nombrado por un nuevo período.

2. Comité de Seguridad de la Información: Es la instancia colegiada que constituye el nexo técnico entre la orgánica de gestión de la Seguridad de la Información y el Gobierno Universitario, teniendo las siguientes funciones:

- Aprobar y actualizar las políticas de Seguridad de la Información para mantenerlas alineadas con los objetivos estratégicos de la Universidad.
- Solicitar y proponer la provisión de recursos para ejecutar proyectos de Seguridad de la Información.
- Supervisar el estado de adopción de las políticas de seguridad en la comunidad universitaria.

La conformación de este comité debe considerar un cuerpo permanente de 8 miembros, que sesione al menos semestralmente o cuando aparezcan incidentes graves que comprometan servicios críticos de la Universidad. El comité podrá invitar a integrantes eventuales o especialistas según sea la necesidad de apoyo para la toma de decisiones.

El Comité estará conformado por las siguientes autoridades:

- **CISO:** Coordina el comité, define la estrategia, reporta al nivel superior.
- **Prorector/a:** Representa al Gobierno Universitario; asegura alineación con la estrategia institucional.
- **Director/a Estratégico/a Informático/a:** Es el responsable de los sistemas TI, soporte técnico y ejecución de medidas.
- **Director/a Jurídico/a:** Brinda asesoría en materias de cumplimiento normativo y protección de datos personales.
- **Secretario/a General:** Actúa como ministro/a de fe de las sesiones del Comité.
- **Contralor/a Universitario/a:** Ejerce supervisión y auditoría de cumplimiento en el contexto del control interno.
- **Director/a de Gestión de Personas:** Participa en la definición de roles, perfiles, planes de capacitación y medidas disciplinarias asociadas.
- **Académico/a experto/a en Seguridad de la Información:** Representa la perspectiva académica y técnica, aporta conocimiento actualizado en ciberseguridad, tecnologías emergentes y buenas prácticas, y asesora en la toma de decisiones estratégicas desde una mirada interdisciplinaria.

Cada miembro del Comité podrá designar un/a representante que asista en su nombre y representación a las sesiones.

El Comité contará con una Secretaría Técnica que levantará acta de las sesiones que se celebren, coordinará las citaciones a las mismas y velará por los aspectos administrativos de la instancia. Dicha función recaerá en un/a funcionario/a designado por el CISO.

- 3. Responsables de la Información:** Son todos los miembros de la comunidad universitaria que tienen la responsabilidad de clasificar los activos de información que pertenecen a sus procesos y autorizar o denegar el acceso a ellos.

V. ACTUALIZACIÓN Y SEGUIMIENTO

Artículo 11: El Comité de Seguridad de la Información reevaluará la Política General de Seguridad de la Información, actividad que será realizada cada dos (2) años, o si se produce algún cambio notable en las tecnologías, en el personal o de existir algún evento que lo amerite.

Además, la revisión de cumplimiento y eficacia de esta política y de las normas establecidas para el uso y la protección de sus activos de información, se realizará una (1) vez al año o si se produce algún cambio notable en las tecnologías, el personal o de existir un evento que lo amerite.

VI. INCUMPLIMIENTO Y RESPONSABILIDAD

Artículo 12: Será considerado como falta a los deberes funcionarios o estudiantiles, realizar acciones que sean contrarias a esta política, que vulneren los servicios y sistemas de información o infraestructura tecnológica de la Universidad.

Todo incidente de seguridad, en virtud de lo anteriormente expuesto, deberá ser comunicado inmediatamente a la autoridad correspondiente, teniendo en consideración el siguiente orden de preferencia:

1. En primera instancia, al/la Oficial de Seguridad de la Información y Ciberseguridad (CISO).
2. En caso de gravedad, también deberá ser informado al:
 - a) Comité de Seguridad de la Información, si está en funcionamiento;
 - b) Dirección Estratégica Informática (DEI), como unidad técnica;
 - c) Y sí corresponde, al Ministerio Público, CSIRT Nacional (ANCI) o Agencia Nacional de Protección de Datos (ANPD).

Para tales efectos, se creará un canal formal de notificación (ciberseguridad@usach.cl), y los tiempos de respuesta variarán según criticidad.

En el mismo sentido, en caso de existir un incidente de esta naturaleza, la Universidad adoptará las medidas tendientes a perseguir las responsabilidades administrativas y disciplinarias y remitirá los antecedentes al Ministerio Público para efectos de la investigación penal pertinente.

Los miembros de la Comunidad Universitaria se obligan a seguir las directrices técnicas de seguridad que imparta la institucionalidad de la Universidad creada al efecto, al resguardo de la información a la que tienen acceso y al tratamiento de datos de conformidad a las políticas e instrucciones institucionales y disposiciones legales sobre la materia que resulten aplicables.

VII. ANEXO I: MARCO LEGAL, REGULATORIO Y NORMATIVO EN MATERIAS DE SEGURIDAD DE LA INFORMACIÓN

- Ley 18.834: Estatuto Administrativo.
- Ley 18.575: De Bases Generales de la Administración del Estado.
- Ley 19.880: Establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.
- Ley 21.663: Ley Marco de Ciberseguridad.

- Ley 21.719: Regula la protección y tratamiento de datos personales, creando la Agencia de Protección de Datos Personales.
- Ley 21.459: Ley de delitos informáticos.
- Ley 17.336: Propiedad Intelectual.
- Ley 19.799: Firma Electrónica.
- Ley 21.180: Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Ley 21.464: Modifica diversos cuerpos legales, en materia de transformación digital del estado
- Ley 20.285: Sobre acceso a la información Pública.
- Decreto Supremo 890/1975: que fija texto actualizado y refundido de la ley 12.927.
- Decreto Supremo 83/2005 Norma técnica para los Órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Decreto Supremo 93/2006, Norma Técnica para Minimizar la Recepción de Mensajes Electrónicos no deseados en las casillas electrónicas de los Órganos de la Administración del Estado y de sus funcionarios.
- Decreto Supremo 7/2023: Establece norma técnica de Seguridad de la Información y Ciberseguridad conforme a la ley 21.180.

VIII. ANEXO II: GLOSARIO DE TÉRMINOS ESPECÍFICOS

Ciberseguridad: La seguridad informática, también conocida como Ciberseguridad, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente los datos y la información contenida en una computadora y/o en un sistema de almacenamiento dedicado, primario o secundario, y/o circulante a través de las redes de computadoras.

Corresponde a un conjunto de acciones, tecnologías, procesos y políticas destinadas a proteger la confidencialidad, integridad y disponibilidad de los sistemas de información, redes y servicios ante amenazas digitales, asegurando la continuidad de funciones esenciales del Estado y la sociedad. Este enfoque integral abarca:

- Servicios esenciales, tanto digitales como presenciales, que deben ser protegidos frente a interrupciones.
- Personas, cuya concientización, formación y gestión de accesos son clave para reducir riesgos humanos.
- Activos no digitales (documentos, dispositivos, infraestructura física), que también forman parte del ecosistema de seguridad.
- Sistemas informáticos, que deben mantenerse seguros y operativos durante todo su ciclo de vida.

Protegiendo la tecnología, procesos, personas y activos físicos, con el fin de garantizar la resiliencia institucional y social frente a amenazas digitales.

Activo de Información: La información y los recursos que la soportan y la procesan y que contiene un valor pertinente para la organización y pueden ser mantenidos en papel o en

medios digitales. Corresponde a elementos que tienen valor para la organización y que se usan para procesar, almacenar o transmitir información. Esto incluye:

- Datos digitales y físicos (ej. archivos, bases de datos, formularios impresos)
- Sistemas informáticos (hardware, software, redes)
- Infraestructura técnica (servidores, UPS, cableado)
- Personas (usuarios, administradores, operadores)
- Servicios institucionales que dependen de la información para su funcionamiento.

Confidencialidad: Es la propiedad de la información que garantiza que solo las personas, sistemas o procesos autorizados puedan acceder a ella. Su objetivo es prevenir el acceso no autorizado, la divulgación indebida o el uso malicioso de datos, ya sean digitales o físicos.

Integridad: Es la propiedad que asegura que la información se mantiene completa, exacta y sin alteraciones no autorizadas durante su generación, transmisión, almacenamiento o procesamiento. También se refiere a la confiabilidad de los sistemas y procesos que manipulan dicha información.

Disponibilidad: Es la garantía de que la información, los sistemas y los servicios estén accesibles y operativos para los usuarios autorizados cuando se necesiten. Esto incluye medidas de continuidad operativa, recuperación ante desastres, y resistencia frente a incidentes o fallos.

Riesgo: Es la posibilidad de que una amenaza aproveche una vulnerabilidad, provocando un impacto negativo sobre los activos de información, los servicios o las personas. Se evalúa como una combinación de la probabilidad de ocurrencia y la magnitud del daño o consecuencia, y es gestionado mediante medidas de prevención, mitigación, transferencia o aceptación.

Comunidad Universitaria: Es el conjunto de personas que poseen un vínculo institucional, a cualquier título, de carácter más o menos permanente, con la Universidad de Santiago de Chile.

2. DERÓGASE la Resolución Exenta N° 1938, de 2020, que Aprueba Política General de Seguridad de la Información.

3. PUBLÍQUESE la presente resolución, una vez totalmente tramitada, en el sitio electrónico de la Universidad, específicamente en el banner “Actos y Resoluciones con efecto sobre terceros”, con el objeto de dar cumplimiento a lo previsto en el artículo 7° de la Ley 20.285 sobre Acceso a la Información Pública y en el artículo 51° de su reglamento.

ANÓTESE Y COMUNÍQUESE,

**DR. RODRIGO VIDAL ROJAS
RECTOR**

Distribución:

- 1. Rectoría;
- 1. Prorectoría
- 1. Dirección Estratégica Informática
- 1. Contraloría Universitaria
- 9. Facultades
- 7. Vicerrectorías
- 1. Secretaría General
- 1. Dirección Jurídica,
- 1. Departamento de Promoción del Cumplimiento
- 1. Unidad de Probidad y Transparencia
- 1. Unidad de Partes, Informaciones y Archivo