EXENTO

REPÚBLICA DE CHILE
UNIVERSIDAD DE SANTIAGO DE CHILE
SECRETARÍA GENERAL
DIRECCIÓN JURÍDICA

APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.

SANTIAGO, 19/06/2020 - 1938

VISTOS: El DFL Nº 149 de 1981, del Ministerio de Educación; la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; la Ley N°19.880, Establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado; la Ley N°20.285, sobre Acceso a la Información Pública; y la Resolución Nº 7 de 2019, de la Contraloría General de la República.

CONSIDERANDO:

a) Que, para la Universidad de Santiago de Chile los activos de la información poseen gran valor, por ello necesitan ser protegidos adecuadamente para que la misión institucional no se vea perjudicada.

b) Que, en ese sentido, resulta de suma importancia proteger la confidencialidad, integridad y disponibilidad de los activos de información, a fin de garantizar la continuidad de los procesos y eliminar o minimizar el daño que se les pudiera producir a estos activos.

c) 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.

RESUELVO:

1. APRUÉBASE la política general de seguridad de la información, cuyo texto es el siguiente:

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDOS

I. Declaración Institucional

La Seguridad de la Información de la Universidad de Santiago de Chile (USACH), es el conjunto de definiciones y acciones destinadas a proteger la confidencialidad, integridad y disponibilidad de los activos de información, a fin de garantizar la continuidad de los procesos de la Institución y eliminar o minimizar el daño que se les pudiera producir a estos activos.

Los niveles básicos de los activos de información corresponden a lo siguiente:

La información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.).
Los equipos, sistemas e infraestructura que soportan a dicha información.
Las personas que utilizan la información y que tienen el conocimiento de los procesos institucionales.
Edificios, instalaciones y demás inmuebles propiedad del servicio u ocupados por ella.
Capital intelectual de la USACH.
Reputación, credibilidad y viabilidad de la USACH.

Dado que los activos de la información poseen valor para la organización necesitan, por tanto, ser protegidos adecuadamente para que la misión institucional no se vea perjudicada.

Esto implica identificar riesgos, detectar vulnerabilidades y establecer los controles de seguridad que sean necesarios, tanto a nivel de Gobierno institucional y de gestión de procesos, como también a nivel de tecnologías de la información.

Las nuevas tecnologías, el desarrollo del conocimiento, la liberación de las comunicaciones, la interoperabilidad y la posibilidad de acceso libre a diversas aplicaciones, requieren de un sistema que permita gestionar la Seguridad de la Información, el cual consiste en la realización de tareas enfocadas en garantizar niveles de Seguridad óptimos para la organización.

La Universidad debe realizar los esfuerzos necesarios para asegurar que todo el personal reciba entrenamiento permanente en seguridad de la información, de acuerdo a su función y rol en la organización.

La Universidad debe realizar los esfuerzos necesarios para gestionar de manera correcta y oportuna la Seguridad de la Información en la organización.

Los riesgos que se identifiquen deberán ser gestionados por la Universidad de manera que sean llevados a un nivel aceptable para el servicio. Para esto podrán ser aceptados, evitados, compartidos o mitigados.

Para aquellos riesgos que no sean aceptables, deberán tomarse las medidas de protección apropiadas, las cuales serán sometidas a la aprobación de la Universidad para asegurar que: Son suficientes para llevar el riesgo a un nivel apropiado; tienen un costo apropiado al beneficio que aporta y reciben los recursos y el apoyo necesario para su implementación.

II. Ámbito Específico

La Política General de Seguridad de la Información de la Universidad de Santiago de Chile establece directrices y define los criterios esenciales, para las acciones y normativas relacionadas con la seguridad de la información.

III. Referencia Normativa

- Ley N°18.834, Estatuto Administrativo.
- Ley N°18.575, de Bases Generales de la Administración del Estado.
- Ley N°19.223 sobre figuras penales relativas a la informática.
- Ley N°19.628, Ley sobre Protección de la Vida Privada.
- Ley N°17.336, Propiedad Intelectual.
- Ley N°19.799, Firma electrónica, 2002.
- Ley N°19.880, Establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del estado.
- Ley N°19.882, Regula nueva política de personal a los funcionarios públicos que indica.
- Ley N°19.927, Ley que modifica códigos penales en materia de delitos sobre pornografía infantil.
- Ley N°20.212, Modifica las leyes N° 19.553, N° 19.882, y otros cuerpos legales, con el objeto de incentivar el desempeño de funcionarios públicos.
- Ley N°20.285, sobre Acceso a la Información Pública.
- DS N°83/2005 Norma técnica para los Órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos
- DS N°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.
- DS N°100/2005 Fija el texto refundido, coordinado y sistematizado de la constitución política de la república de Chile.
- DS N°890/1975, Sobre seguridad del Estado.
- Jurisprudencia administrativa y judicial sobre uso de correos electrónicos
- NCH 27001 y 27002.

IV. Objetivos de la Gestión de Seguridad de la Información

- Establecer mecanismos apropiados que garanticen la seguridad de los activos de información del Servicio de la Institución.
- Representar los intereses de la Universidad, con respecto a la administración y utilización, que los usuarios internos y/o externos deben hacer de los activos de información de la Institución, así como de las medidas que se deben adoptar para la protección de dichos recursos.
- Especificar las medidas esenciales de seguridad de la información que el servicio debe adoptar, para resguardarse apropiadamente contra amenazas que podrían afectar la confidencialidad, integridad y disponibilidad de la información, ocasionando alguna de las siguientes consecuencias: pérdida o mal uso de los activos de información, pérdida de imagen Institucional y pérdida de información sensible.
- Asegurar que los recursos humanos, económicos, tecnológicos y procesos críticos de la operación estén apropiadamente protegidos por sus responsables, con el fin de minimizar los riesgos que puedan afectar el bienestar de las personas y la continuidad de la operación.
- Asegurar que estas protecciones se realicen de una manera consistente con la operación, flujo de trabajo y normativas vigentes del servicio.
- Definir las acciones y directrices a realizar para la clasificación y catastro de activos de información.

- Definir las acciones necesarias para el análisis de riesgo de acuerdo a la normativa vigente en la institución.
- Definir y planificar las acciones a realizar para la capacitación del personal.
- Establecer la estructura para el marco de políticas, estándares y procedimientos en materia de seguridad de la información a ser desarrollados en la institución.

V. Principios

Será política de la Universidad de Santiago de Chile (USACH), establecer principios generales de seguridad de los recursos, los que deben permanecer estables a través del tiempo para el cumplimiento por parte de todo el personal del servicio y/o Comunidad Universitaria.

Dichos principios se describen a continuación:

1. Integridad y exactitud:

Se debe garantizar que toda la información, transacciones y operación se encuentren libres de errores y/o irregularidades de cualquier índole. Es responsabilidad de cada funcionario generador de datos, la exactitud de estos al momento de su ingreso a cualquier sistema de información organizacional. Es responsabilidad del funcionario responsable de los sistemas que los contienen una vez ingresados, la integridad de estos durante todo su procesamiento y mantención en repositorios de consulta.

2. Legalidad:

Las operaciones deben cumplir con las reglamentaciones legales vigentes. Es responsabilidad indelegable de cada funcionario el velar por el cumplimiento de este principio en su ámbito de competencia, debiendo resolver cualquier duda ante las instancias pertinentes.

3. Disponibilidad:

Se debe garantizar que las operaciones críticas no tengan interrupciones que pongan en riesgo la continuidad de dicha operación. Es tarea de cada responsable de la administración de la información, sistema o proceso según sea el caso, el cumplir permanentemente con este principio e informar a las instancias que corresponda, sin dilación, su potencial incumplimiento y es responsabilidad del área informática garantizar la continuidad de los servicios informáticos.

4. Confidencialidad:

Se debe garantizar que toda información (física y digital) y sus medios de procesamiento y/o conservación, estén protegidos del uso no autorizado o revelaciones accidentales, errores, fraudes, sabotajes, espionaje industrial, violación de la privacidad y otras acciones que pudieran perjudicarla. Es tarea de cada responsable de repositorio de datos digitales, funcionario con acceso permanente o accidental a documentación física que contenga información del servicio, o administrador de seguridad de la Información, el cumplir irrestrictamente con este principio y con la legislación correspondiente.

5. Salvaguarda Física:

Todos los recursos deben contar con medidas de protección física que eviten el acceso y/o utilización indebida por personal no autorizado. La custodia permanente o circunstancial de los bienes Institucionales por parte de cada funcionario, debe propender al cumplimiento de este principio.

6. Propiedad:

Todos los derechos de propiedad de la USACH deben estar adecuadamente establecidos y protegidos. Será responsabilidad de cada gestor de procesos, productos o iniciativas que contengan o generen derechos de propiedad, velar por el cumplimiento de este principio.

VI. Alcance o amplitud de la Política de Seguridad de la Información

Esta política debe ser conocida y aplicada por todos quienes trabajan y colaboran en la Universidad de Santiago de Chile (USACH), en cualquier nivel jerárquico, ya sean funcionarios de planta, a contrata u honorarios, o en cualquier calidad que se desempeñen en la institución siendo parte de la Comunidad Universitaria, así como a los proveedores o terceros autorizados a acceder a los sistemas o, en definitiva, cualquiera que use los activos de información de la Institución.

Esta política cubre toda la información impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos, mostrada en videos o registros de audio, entre otras. Además, cubre los equipos, sistemas e infraestructura que soportan a dicha información.

En el caso que un proveedor externo inicie sus labores en dependencias de la USACH, deberá firmar un documento donde haga mención del conocimiento de la política de seguridad de información y el cumplimiento de ésta mientras perduren los trabajos.

Esta Política aplica de igual forma a los accesos de conexión remota a favor del desempeño de las funciones de la USACH, se entiende la lectura y envió de correos electrónicos, la vista de los recursos y/o servicios, a través, de los sitios Web establecidos.

Bajo la premisa de garantizar la Seguridad de la Información y que esta por su naturaleza es responsabilidad de todos los usuarios que se relacionen con esta Institución, ya sean usuarios externos, que sean identificables, que presten algún servicio o asesoría y que por sus funciones deban acceder a nuestra Red de Área Extendida (WAN) o nuestros usuarios internos en sus diversas calidades jurídicas haciendo uso de la Red de Área Local (LAN).

VII. Re evaluación y Cumplimiento

Una de las tareas que deberán ser ejecutadas por el Comité de Seguridad de la Información de la USACH, es la reevaluación de la presente Política.

Esta actividad deberá ser realizada una vez al año o si se produce algún cambio notable en las tecnologías, en el personal o de existir un evento que lo amerite.

Así también, se deberá programar la revisión de cumplimiento y efectividad de la Política General de Seguridad de la Información y de cada una de las normas establecidas en el uso de los activos de información de propiedad de la USACH una vez al año o si se produce algún cambio notable en las tecnologías, en el personal o de existir un evento que lo amerite, donde se deberán revisar los incidentes ocurridos y proponer planes de mejoras en los casos necesarios.

VIII. Difusión

La Política General de Seguridad de la Información al igual que las Políticas de Seguridad Especificas, Normas, Planes, deberán ser difundidos con el objetivo que estas sean conocidas y además implementadas por todo el personal, los medios de difusión serán definidos mediante un plan anual de "Difusión, Sensibilización y Capacitación" a Nivel Institucional, el cual será actualizado anualmente o según corresponda. Este plan será realizado en conjunto por las unidades que corresponda según sus competencias y atribuciones específicas.

IX. Reglas de la Política

1. *La Universidad de Santiago de Chile (USACH) reconoce a la información, los sistemas de información y recursos asociados a ella, como activos críticos de la Institución, por lo que deben ser administrados con el mismo rigor que el resto de los activos de esta.*

2. *La información debe ser protegida de manera adecuada, en concordancia a la definición de su sensibilidad y valor, resguardando su confidencialidad, integridad y disponibilidad. Para realizar esta protección, es necesario identificar y clasificar los activos de información, los sistemas de información y recursos asociados. La información debe ser protegida sin hacer exclusiones en base a su presentación, almacenamiento, los sistemas que la procesen y los métodos de transporte que se utilicen.*

3. *La Seguridad de la Información es responsabilidad de todos quienes se desempeñan en la USACH, independientemente de su nivel jerárquico y de su calidad jurídica, requiriendo del apoyo, participación y compromiso de las jerarquías superiores de la institución. Es obligación de todas estas personas, informar de cualquier actividad, situación anómala o incidente que eventualmente pueda atentar contra la Seguridad de Información.*

4. *La información de la institución no debe quedar disponible a personas o entidades externas, salvo en las situaciones y formas expresamente establecidas en las leyes y normas vigentes, y con controles que garanticen su protección. Cuando sea requerido una declaración de la autoridad para dar estos accesos, esto debe estar expresamente definido en las políticas o procedimientos relacionados.*

5. *Cada funcionario o colaborador de la Institución debe acceder sólo a la información que le es necesaria para cumplir sus funciones y tiene la obligación de notificar cualquier actividad o situación que contravenga estos lineamientos.*

6. *La USACH reconoce que la sensibilización, capacitación y entrenamiento adecuados de su personal en las materias de Seguridad de la Información son tareas prioritarias. Por ello, se establecen las instancias de capacitación, entrenamiento y divulgación en un Plan Anual.*

7. *La Institución declara cumplir con la normativa vigente, la Ley N° 20.285 junto con toda la legislación aplicable a la información y las normas de los organismos fiscalizadores, relacionadas con aspectos de reserva y privacidad de la información.*

8. *Se establece la creación de un Comité Seguridad de la Información que tiene por objeto velar por la existencia de las medidas de seguridad destinadas a proteger y preservar los activos de información de la Institución, que se materializan en las políticas, procedimientos y estándares en la materia, teniendo la autoridad para su implementación y control.*

9. *De esta política general se desprende el Manual de Seguridad de la Información y sus documentos asociados, que juntos constituyen la definición del marco normativo de seguridad de la USACH, haciendo hincapié en el rol que le corresponde asumir a todos los funcionarios y colaboradores de la institución, para lograr el resguardo permanente de la información y los recursos asociados.*

10. *El incumplimiento del marco normativo de seguridad de la información de la USACH será sancionado en su mérito.*

11. *La implantación y la aplicación de las medidas de seguridad que se definan corresponde a todas las unidades de la institución.*

12. *La verificación del cumplimiento de esta política general y del Manual de Seguridad de la Información será realizada por las unidades definidas por la Institución.*

13. *La USACH reconoce como uno de sus atributos estratégicos la continuidad de sus Servicios, para lo cual compromete recursos para la generación, mantención y pruebas periódicas de un Plan de Continuidad de Servicios.*

X. Roles y Funciones

Los roles relevantes para el cumplimiento de esta política y sus funciones principales son los siguientes:

Rol	Responsabilidad
Comité de Seguridad de la Información	• Responde ante el Jefe de Servicio, por la existencia y cumplimiento de las medidas orientadas a mantener un nivel de seguridad de la información acorde con las necesidades del Servicio y los recursos disponibles. • Tener a cargo el desarrollo inicial de las Políticas de Seguridad de la Información al interior de la Institución, el control de su implementación y velar por su aplicación. • Coordinar la respuesta institucional ante incidentes de Seguridad Mayor. • Supervisar la implementación de procedimientos y estándares que se desprendan de las Políticas de Seguridad de la Información. • Arbitrar conflictos en materia de Seguridad de la Información y los riesgos asociados a ellas. • Coordinarse con los Comités de Calidad y de Riesgos de la Institución para mantener lineamientos y estrategias comunes de gestión. • Crear el Manual de Seguridad de la Información.
Actor de Auditoria Interna	• Monitorear el avance de cada una de las etapas de la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI).
Roles de la Institución	• Tienen la responsabilidad de cumplir con lo establecido en este documento y aplicarlo tanto en su entorno laboral, como fuera de éste. Además, tiene la obligación de alertar de manera oportuna y adecuada por los canales y procedimientos formalmente establecidos, cualquier situación que pueda poner en riesgo la seguridad de la información. • Deben participar activamente en la definición del valor de la información para el servicio, de manera que se puedan definir los controles apropiados para protegerla. • En su rol de propietario de la Información: Es responsable por la protección de la información a su cargo, por la designación del custodio de la información, es quien tiene y puede cambiar las características en la clasificación de los elementos de información.

Rol	Responsabilidad

	• En su rol de custodio de la Información: (cualquier persona que mantiene bajo su responsabilidad, información de la cual no es el Propietario). Es responsable de aplicar las medidas de seguridad que se definan de acuerdo al valor de los activos. En esta categoría se encuentra:
	  ○ El personal encargado de los sistemas de tecnologías de información que crean, procesan o modifican la información del servicio y sus usuarios externos.
	  ○ El personal que tiene acceso a información del servicio y sus usuarios externos.
	• Además, tienen la responsabilidad de cautelar el cumplimiento de las medidas de control definidas.
	• Y acatar las definiciones de seguridad, en torno a políticas, normas o procedimientos de seguridad de la información

Encargado de Seguridad de la Información	• Apoyar al Comité de Seguridad de la Información (CSI) de la Institución en la definición de las medidas de protección necesitadas.
	• Coordinar actividades para las sesiones del CSI.
	• Es el representante del Gobierno Central en la definición y aplicación de los criterios de seguridad de la información en el Servicio, para lo cual:
	  ○ Debe validar que los activos de información son identificados y valorizados apropiadamente por sus Propietarios, y que este valor se mantiene actualizado en el tiempo.
	  ○ Debe analizar permanentemente el nivel de riesgo existente, proponiendo soluciones efectivas.
	• Una vez autorizada la implementación de las medidas de protección, debe coordinar con los encargados respectivos su materialización correcta y oportuna,
	• Alinear la debida respuesta y priorización al tratamiento de incidentes y riesgos vinculados a los activos de información de los procesos institucionales y sus objetivos de negocio.
	• Monitorear el avance general de las implementaciones con respecto a estrategias de control y tratamiento de riesgos.
	• Monitorear el cumplimiento de normas, políticas y procedimientos de Seguridad de la Información.
	• Monitoreo del cumplimiento de las acciones que sustentan la gestión de los Planes de Recuperación Tecnológico (PRT) y los Planes de Continuidad del Servicio (PCS).
	• Gestión y monitoreo de las directrices de Seguridad de la Información relativas al cumplimiento regulatorio.

Rol	Responsabilidad
	• Monitorear el avance general de la implementación de estrategias de control y tratamiento de riesgos, • Contribuir al cumplimiento de los compromisos para el Programa de Seguridad de la Información.

XI. Marco General para las Políticas de Seguridad de la Información

El marco general que se utilizará para la gestación de las políticas es el siguiente:

- Definición de la Seguridad de la Información
- Objetivos Políticas de Seguridad
- Formato de las Políticas
- Gestación de una Política
- Aprobación de Políticas
- Difusión de las Políticas
- Revisión de las Políticas

XII. Sanciones

El marco general que se utilizará para la gestación de las políticas es el siguiente:

Toda infracción a las Políticas de Seguridad de la Información, como así mismo cualquier denuncia a este tipo de conductas, referente a funcionarios de la Universidad de Santiago de Chile, debe ser investigada y/o denunciada ante la Jefatura correspondiente, debiéndose aplicar las sanciones administrativas que procedan y/o ejerciendo las acciones civiles y penales que correspondan conforme a la magnitud y características del incumplimiento de esta.

XIII. Marco Normativo de Seguridad de la Información

Esta Política General de Seguridad fue construida bajo la norma ISO/IEC 27.001 referida a la Seguridad de la información y homologada en la NCH 27.001, en la cual se establece cubrir los siguientes dominios, conformando cada uno de ellos al menos una Política específica:

1. Política de Seguridad de la Información
2. Organización de Seguridad de la Información
3. Gestión de Activos
4. Seguridad de los Recursos Humanos
5. Seguridad física y ambiental
6. Gestión de Operaciones y Comunicaciones
7. Control de Acceso
8. Mantención, Desarrollo y Adquisición de Sistemas
9. Gestión de Incidentes de Seguridad de la Información
10. Gestión de Continuidad
11. Cumplimiento con requerimientos legales

XIV. Enmienda, modificación y anulación

El Comité de Seguridad de la Información. Puede enmendar, modificar o anular esta Política en cualquier momento.

XV. Glosario de Términos Específicos

Los términos y definiciones que se presentan en esta sección son aplicables a esta política específica, y son primordiales para el buen entendimiento y aplicación del Sistema de Gestión de Seguridad de la Información:

a) **Activo de Información**: Son todos aquellos elementos ((papel, digital, texto, imagen, audio, video, etc.) que contengan información relevante para el negocio relacionados a la producción, emisión, almacenamiento, comunicación, visualización y recuperación de valor para La USACH.
b) **Documento Electrónico**: De acuerdo a la Ley 17.779, es toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenados de un modo idóneo para permitir su uso posterior.
c) **Confidencialidad**: Asegurar que la información sea accesible solo para aquellos usuarios autorizados para tener acceso.
d) **Integridad**: Salvaguardar que la información y los métodos de procesamiento sean exactos y completos.
e) **Disponibilidad**: Asegurar que los usuarios autorizados tengan acceso a la información y bienes asociados cuando lo requieran.
f) **Seguridad de la Información**: Todas aquellas medidas preventivas y reactivas que permitan resguardar y proteger la información buscando mantener la confidencialidad, integridad y disponibilidad de la misma.
g) **Riesgo**: Es la combinación de la probabilidad de ocurrencia de un evento o incidente y su impacto en la organización.
h) **Probabilidad**: Es la oportunidad de que algo ocurra. Es la medición de la oportunidad.
i) **Impacto**: Efecto causado en los objetivos de la USACH.
j) **Evento**: Una ocurrencia identificada en un sistema, servicio, o cualquier otro elemento. Es una posible brecha de cumplimiento de las Políticas, normas, procedimientos o fallas en las medidas de seguridad ya implementadas.
k) **Incidente**: Esta indicado por un simple o múltiples eventos no esperados. Esto tiene una lata probabilidad de comprometer la continuidad de las operaciones de la misión institucional.
l) **Amenaza**: evento que puede desencadenar un incidente en la organización, produciendo eventualmente daños materiales o perdidas inmateriales en los activos de información.
m) **Vulnerabilidad**: Una debilidad que facilita la materialización de una amenaza, la situación generada, dependerá del contexto encontrado,
n) **PRT**: Planes de recuperación Tecnológico, es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.
o) **PCS**: Planes de Continuidad del Servicio, el cual tiene como objetivo mantener la funcionalidad de una organización, a un nivel mínimo aceptable durante una contingencia.

2. 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", a objeto de dar cumplimiento a lo previsto en el artículo 7° de la Ley N°20.285 sobre Acceso a la Información Pública y en el artículo 51 de su Reglamento.

ANÓTESE Y COMUNÍQUESE.

DR. JUAN MANUEL ZOLEZZI CID, RECTOR.

Lo que transcribo a usted, para su conocimiento.

Saluda a usted,

UNIVERSIDAD DE SANTIAGO DE CHILE SECRETARIO GENERAL

GUSTAVO ROBLES LABARCA
SECRETARIO GENERAL

JMZC/GRL/AJT
Distribución
1.- Secretaría General
1.- Dirección Jurídica
1.- Dirección de Desarrollo Institucional
1.- Archivo Central
1.- Oficina de Partes