UNIVERSIDAD DE CHILE
Vicerrectoría de Asuntos Económicos y Gestión Institucional

UNIVERSIDAD DE CHILE - CONTRALORIA INGRESO 27 NOV 2013

UNIVERSIDAD DE CHILE LEGALIDAD CONTROLADA 29 NOV 2013 CONTRALORIA

APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIVERSIDAD DE CHILE

RESOLUCIÓN EXENTA N° 01682

Santiago, 27. 11. 2013.

VISTOS:

Lo dispuesto en el D.F.L Nº 3 de 2.006 del Ministerio de Educación, y en el D.U. Nº 249, de 2.013; lo dispuesto en el Decreto Supremo N°83 de 2005, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos, lo señalado en la Resolución N°1600 de la Contraloría General de la República, y

CONSIDERANDO:

1. Que la Vicerrectoría de Asuntos Económicos y Gestión Institucional, tiene bajo su dependencia a la Dirección de Servicios de Tecnologías de Información y Comunicaciones cuyo quehacer está orientado a prestar servicios especializados en tecnologías de información y comunicaciones, buscando permanentemente nuevas y mejores prácticas en donde éstas propicien un cambio, con el objeto de apoyar a la Universidad de Chile en la realización eficiente de sus labores y servicios, y

2. Que se hace necesario establecer los requisitos y condiciones generales de seguridad de la información a las que se encuentra sujeta la Universidad de Chile en cuanto a esta materia, de acuerdo a las normas legales y reglamentarias pertinentes, los riesgos a que están expuestos sus activos de información y los principios y objetivos internos para el resguardo de sus operaciones, así como establecer normas que regulen el correcto uso de los servicios de información a través de las distintas actividades que el personal de la Universidad realiza en el desempeño de sus funciones, con el fin de asegurar la confidencialidad, integridad y disponibilidad de los servicios de información

RESUELVO:

1. Apruébese la Política General de la Seguridad de la Información para la Universidad de Chile, que es del tenor siguiente:

POLÍTICA GENERAL
DE SEGURIDAD DE LA INFORMACIÓN
Universidad de Chile

1. Introducción

La seguridad de la información es un activo que, como otros activos de la Universidad de Chile, es esencial para la operación y continuidad de los servicios y requiere en consecuencia una protección adecuada.

En este contexto, se vuelve necesario definir lineamientos claros en materia de seguridad de la información de acuerdo al marco normativo vigente, a saber la Ley 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma y los siguientes decretos supremos:

D.S. 83: Norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.

Para el cumplimiento de lo dispuesto anteriormente, la Universidad de Chile se apoyará en la Norma Chilena Oficial NCh-ISO 27002.Of2009.

La utilización de la norma indicada anteriormente, basada en la norma internacional ISO/IEC 27002:2005, permitirá la absorción de prácticas para la gestión de la seguridad de la información, de forma de asegurar su correcto tratamiento.

2. Declaración Institucional

La seguridad de la información es de responsabilidad de todos los organismos de la Universidad, por lo cual se crea el Comité TI, integrado por representantes de todas las facultades, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas tecnológicas y de seguridad.

Dicho Comité contará con un coordinador, quien cumplirá la función de promover e impulsar la implementación de la presente política, la cual estará siempre alineada con la misión y la visión de la Universidad de Chile.

La Universidad de Chile facilitará las herramientas, acceso a servicios y condiciones que permitan ejecutar la labor propia de cada miembro de la comunidad universitaria.

Dichos servicios deben ser utilizados en materias relacionadas directamente con la respectiva función de cada miembro de la comunidad universitaria o con el quehacer propio de la Universidad de Chile. En este sentido, se establece que los usuarios no podrán hacer uso de los sistemas o herramientas para propósitos personales de carácter comercial, con fines políticos u otro que no tenga relación con el ámbito universitario.

Cada miembro de la comunidad universitaria, tiene la responsabilidad de proteger la información confidencial de la universidad. El uso inapropiado de la información confidencial, expone a la Universidad de Chile a riesgos de seguridad como filtración de información sensible, suplantación de identidad, accesibilidad a los servicios, litigios por aspectos legales, entre otros.

La autoridad que suscribe, hace suyo el compromiso de velar por el cumplimiento de los objetivos de Gestión de Seguridad de la Información y de difundirlos por los medios disponibles y accesibles entre toda la comunidad universitaria, de tal forma que cada organismo sea responsable de su correcta implementación y cumplimiento.

3. Objetivos de la Gestión de Seguridad de la Información

Objetivo General

La correcta implementación de esta Política de Seguridad de la Información, permite identificar una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos, los cuales buscan que los activos de información cumplan las siguientes condiciones:

- **Integridad:** La información está completa, actualizada y es veraz, sin modificaciones inapropiadas o corrupción.
- **Confidencialidad:** La información está protegida de personas/usuarios no autorizados.

- **Disponibilidad:** Los usuarios autorizados pueden acceder a las aplicaciones y sistemas cuando lo requieran para utilizar la información apropiadamente al desempeñar sus funciones.

Objetivos Específicos

- Realizar un catastro de activos de información, definiendo los procesos propios de cada facultad/organismo que estén involucrados con estos activos.
- Analizar los riesgos que permitan diseñar y establecer medidas que los disminuyan y que estén de acuerdo a la normativa vigente.
- Capacitar a toda la comunidad universitaria, sobre su responsabilidad en el cumplimiento de los objetivos establecidos en esta Política de Seguridad de la Información y su alcance, así como la incorporación progresiva de buenas prácticas laborales relacionadas con estos.

- Establecer los lineamientos para el marco de la elaboración de políticas, instructivos, estándares y procedimientos en materia de seguridad de la información a ser desarrollados en la Universidad de Chile.
- Realizar evaluaciones y seguimientos permanentes de los eventos que generen impacto en los ámbitos de la seguridad de la información, como también analizar y aplicar las oportunidades de mejora que sean identificadas.
- Establecer los medios y oportunidades de difusión y comunicación de esta política y sus objetivos a todos los niveles de la universidad, los cuales permitan promover el cumplimiento de normas y procedimientos de seguridad.

4. Alcance de la Política General de Seguridad de la Información

La presente política de seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el fin de apoyar eficazmente la gestión de seguridad de la información en los sistemas informáticos y recursos tecnológicos de la Universidad.

Los ámbitos a desarrollar en materia de seguridad de la información, se abordarán en lo relacionado a la definición de documento electrónico y a los sistemas de información vigentes.

Además se deberán elaborar los documentos necesarios para su correcta implementación, considerando al menos los siguientes:

- Política de uso de Red.
- Política de uso aceptable y navegación por Internet.
- Política de respaldos.
- Política de correo electrónico.
- Política de uso de software.
- Política de cuentas de usuarios y contraseñas.

5. Revisión de la Política General de Seguridad de la Información

La presente política deberá ser revisada y actualizada de forma periódica y no podrá exceder de los 3 años como máximo, para asegurar su conveniencia, suficiencia y eficacia continua.

6. Roles y responsabilidades

Responsable	Funciones
Director Servicios de Tecnologías de la Información y Comunicación	Promover la difusión de las políticas, instructivos y procedimientos, asociados a seguridad de la información, que sean aprobados por la Vicerrectoría de Asuntos Económicos y Gestión Institucional. Coordinar y presidir las sesiones y actividades del comité de TI.
Comité de Tecnologías de la Información	Revisar y proponer las políticas asociadas a seguridad de la información en forma permanente, con el objeto de mantenerlas actualizadas en relación a los cambios institucionales.
	Supervisar el estado de la implementación de la política de seguridad de la información.
Oficial de Seguridad de la Información	Proponer y elaborar las políticas de seguridad, efectuar los controles necesarios y velar por su correcta implementación y aplicación.
	Coordinar la respuesta a incidentes de seguridad de la información y riesgos vinculados a los activos de la información.
	Coordinarse con otras instituciones, a fin de mantenerse al tanto de nuevas normativas o estándares a aplicar en términos de seguridad.
	Asesorar en materias de seguridad de la información, normativa y plan de tratamiento de riesgos.
Representantes de Organismos	Velar por el cumplimiento de la presente política de seguridad de la información al interior de su organismo respectivo. Además velar por el correcto tratamiento de la información y la elaboración de políticas específicas.
Alumnos, académicos, autoridades y funcionarios	Manejar de forma segura la información confidencial de la universidad así como también, los recursos provistos para el tratamiento de dicha información. Es obligación de todos y cada uno de los miembros de la comunidad universitaria cumplir a cabalidad lo indicado por la presente política y los reglamentos y procedimientos que de él se desprendan, así como también notificar cualquier actividad anómala que atente contra la confidencialidad, integridad y disponibilidad de la información.

7. Glosario de términos (en orden de mención)

Activo de información: toda la información que tenga valor para la institución, como por ejemplo: documentos digitales y bases de datos, correo electrónico, documentación de sistemas, manuales de usuarios, procedimientos operativos o de soporte, planes de continuidad, configuración del soporte de recuperación, entre otros. Dentro de los activos de información, se puede agregar a su vez a las personas como fuentes o almacenadoras de información no documentada.

Documento electrónico: toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior. (Definición Ley 19.799)

Firma electrónica: es cualquier sonido, símbolo proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor. (Definición Ley 19.799)

Decreto supremo: es un mandato escrito que emana del Presidente de la República en uso de las facultades que ejerce en el marco de la potestad reglamentaria y puede ser modificado o dejado sin efecto mediante otro D.S. (definición derecho administrativo).

Norma: Es un documento de conocimiento y uso público, aprobado por un organismo reconocido. La norma establece, para usos comunes y repetidos, reglas, criterios o características para las actividades o sus resultados y procura la obtención de un nivel óptimo de ordenamiento en un contexto determinado.

Amenaza: representa una fuente potencial de eventos adversos para la seguridad informática.

Sistema de información: es un conjunto organizado de elementos, que pueden ser personas, datos, actividades o recursos materiales en general. Estos elementos interactúan entre sí para procesar información y distribuirla de manera adecuada en función de los objetivos de una organización.

Riesgo: amenaza de impactar y vulnerar la seguridad del documento electrónico y su posibilidad de ocurrencia (definición D.S.N°83).

Proceso: es un conjunto de actividades o eventos coordinados que se realizan bajo ciertas circunstancias con un fin determinado.

Procedimiento: es el modo de ejecutar determinadas acciones que suelen realizarse de la misma forma, con una serie común de pasos claramente definidos.

Incidente de seguridad informática: se define como un evento que atente contra la confidencialidad, integridad y disponibilidad de un documento electrónico o sistema computacional o asimismo el acto de violar explícita o implícitamente una política de seguridad.

2. Una vez tramitada la presente resolución, procédase a su publicación en el portal web institucional, a objeto de dar cumplimiento a lo dispuesto en la ley N°20.285 sobre Acceso a la Información Pública y lo previsto en su reglamento.

ANÓTESE, COMUNÍQUESE Y REGÍSTRESE

UNIVERSIDAD DE CHILE VICERRECTORIA DE ASUNTOS ECONÓMICOS Y GESTIÓN INSTITUCIONAL

PROF. FRANCISCO MARTÍNEZ CONCHA
Vicerrector de Asuntos Económicos
y Gestión Institucional

Distribución:
- Contraloría Universitaria
- Rectoría
- Prorrectoría
- Facultades e Institutos
- Vicerrectorías
- Hospital Clínico Universidad de Chile
- Programa de Bachillerato
- Liceo Manuel de Salas
- Direcciones Nivel Central
- Dirección de Servicios de Tecnologías de Información
- Oficina Central de Partes Archivo y Microfilm.