VICERRECTORÍA
ECONÓMICA Y DE
ADMINISTRACIÓN udp

RESOLUCIÓN Nº 012/2021
VICERRECTORÍA ECONÓMICA Y DE ADMINISTRACIÓN

Santiago, 25 de marzo de 2021

VISTOS:

1. La necesidad de asumir la responsabilidad de implantar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información, el cual permita lograr niveles adecuados de seguridad para todos los activos de información.

2. La búsqueda de prevenir y manejar los riesgos asociados a la administración y uso inadecuado de la información.

3. La necesidad de informar sobre las normas y mecanismos que se deben cumplir y utilizar para proteger la información.

4. Revisado por la Dirección General de Sistemas y la Dirección Jurídica

5. Aprobado por la Vicerrectoría Económica y de Administración

CONSIDERANDO:

1. El artículo 14º letra k) del Reglamento General de la Universidad Diego Portales.

RESUELVO:

1. Aprobar la “Política Global de Seguridad de la Información”, que se adjunta a la presente resolución y que comenzará a regir a contar de esta fecha.

Regístrese y comuníquese,

Pablo Vigneaux Ovalle
Vicerrector Económico y de Administración

DISTRIBUCIÓN:

- Rector
- Vicerrectores
- Dirección Jurídica
- Contraloría
- Decanos
- Directores de Escuelas
- Coordinadores
- Secretarios Académicos
- Secretarios de Estudios
- Comunicad Universitaria

Maria Isabel Diaz
Contralora UDP

Firmado digitalmente por Maria Isabel Diaz
Nombre de reconocimiento (DN): cn=Maria Isabel Diaz, o=UDP, ou=Contraloria, email=mariaisabel.diaz@udp.cl, c=CL
Fecha: 2021.03.25 16:54:25 -03'00'

PVO/pb

Política Global de
Seguridad de la Información

Universidad Diego Portales y relacionadas

Versión 2.0

Marzo 2021

1. Información del Documento

HISTORIA DEL DOCUMENTO			
Nombre del Documento:	PO.05.00.00 – Política Global de Seguridad de la Información		
Generado por:	Oficial de Seguridad de la Información		
Revisado por	Dirección General de Sistemas – Dirección Jurídica	**Fecha de Creación:**	Diciembre 2020
Aprobado por:	Vicerrectoría Económica y de Administración	**Fecha de Aprobación:**	Marzo 2021
Oficializado por:	Contraloría	**Entrada en vigencia:**	Marzo 2021

(*) La presente versión substituye completamente a todas las precedentes, de manera que éste sea el único documento válido.

CONTROL DE VERSIONES			
Versión:	**Última Actualización:**	**Aprobado por:**	**Descripción:**
1.0	Septiembre 2014	Rectoría	Creación y primera versión del documento.
2.0	Enero 2021	Rectoría	1) Actualización de la nomenclatura de documentos desde la versión ISO 270001:2005, a la versión ISO 27001:2013. 2) Incorporación de nuevas reglas en la política asociadas a la protección global, confidencialidad y control sobre los activos de información.

UNIVERSIDAD DIEGO PORTALES
Mª Isabel Díaz
CONTRALORÍA

María Isabel Díaz
Contralora UDP

Firmado digitalmente por Maria Isabel Diaz
Nombre de reconocimiento (DN): cn=Maria Isabel Diaz, o=UDP, ou=Contraloria, email=mariaisabel.diaz@udp.cl, c=CL
Fecha: 2021.03.25 16:26:06 -03'00'

2. Índice

3. Introducción

Universidad Diego Portales, en adelante UDP, es una organización sin fines de lucro con una amplia trayectoria al servicio de una educación de calidad, la cual tiene como principal objetivo académico el formar profesionales con un alto dominio teórico y práctico de su futuro campo laboral, comprometidos con el desarrollo social, económico y cultural del país.

Como tal, UDP y sus relacionadas reconocen la importancia y el valor de la información con respecto al funcionamiento eficiente y efectivo de la organización. La información no es sólo crítica para el éxito de la universidad, sino estratégica para su supervivencia en el largo plazo.

Es por ello que la universidad y sus relacionadas asumen la responsabilidad de implantar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información, en adelante “SGSI”, el cual permita lograr niveles adecuados de seguridad para todos los activos de información considerados relevantes; en este sentido, la organización se propone alcanzar en el mediano plazo (2021-2023) como estándar, estar alineados con la normativa ISO 27001:2013.

4. Objetivos

En su conjunto, las políticas de seguridad de la información de UDP y sus relacionadas, buscan prevenir y manejar los riesgos asociados a la administración y uso inadecuado de la información. También, se espera a través de ellas, informar a los usuarios/as, tales como: alumnos/as, académicos/as, funcionarios/as y personal externo sobre las normas y mecanismos que deben cumplir y utilizar para proteger la información.

Los principales objetivos de esta política, y que contribuyen al logro de los objetivos estratégicos de la universidad y sus relacionadas, son:

4.1. Determinar las medidas esenciales de seguridad de la información que la universidad y sus relacionadas deben adoptar, para protegerse apropiadamente frente a posibles amenazas que podrían afectar de alguna manera la autenticidad, confidencialidad, integridad y disponibilidad de la información, ocasionando algún impacto negativo en la continuidad del proceso, mal uso de los activos de información o pérdida de imagen.

4.2. Asegurar que los recursos humanos, económicos, tecnológicos y procesos críticos de la universidad y sus relacionadas estén adecuadamente protegidos por sus responsables, de manera tal de minimizar los riesgos que puedan afectar el bienestar de las personas y la continuidad de la operación.

4.3. Asegurar que estas protecciones se realicen de una manera consistente con las definiciones que realizan las autoridades universitarias, los flujos de trabajo y las normativas vigentes que afectan a la universidad y sus relacionadas.

4.4. Contar con una organización consciente de sus derechos y deberes, y que participe en forma activa y responsable para que, entre otras cosas, proteja y difunda el buen nombre e imagen de la universidad y sus relacionadas.

4.5. Identificar los riesgos que puedan impactar la disponibilidad, integridad y confidencialidad de la información dentro de la organización, para determinar e implementar medidas de tratamiento para los riesgos identificados.

5. Ámbito de Aplicación y Alcance

Esta política se aplica a los activos de información (información, procesos, sistemas, personas) utilizados por la universidad y su relacionadas, con alcance a todos los/as funcionarios/as, académicos/as y demás integrantes de la universidad, que participan en todos los procesos de la institución, ya sean aquellos que directamente tienen la necesidad de hacerlo, como también aquellos que intervienen en actividades específicas. También aplica al personal externo que preste o prestare servicios, remunerados o no, a la universidad y sus relacionadas.

Adicionalmente, es aplicable a todo activo de información que la universidad y sus relacionadas posea en la actualidad o en el futuro, de manera que la no inclusión explícita dentro del presente documento, no lo excluye del alcance de la presente política.

Por su parte, los capítulos considerados de la norma ISO 27001:2013 dentro de esta política global y sus políticas complementarias, involucran los 14 capítulos de la norma, sin excepción de alguno.

El alcance se extenderá a toda la universidad, las facultades y entidades relacionadas, tales como: Clínica Odontológica UDP S.A., Servicio y Ediciones UDP Ltda., Fundación Fernando Fueyo Laneri y Fundación Centro de Estudios, Servicios y Asesorías UDP.

6. Control y Sanciones

El incumplimiento en la aplicación de lo dispuesto en la presente política debe ser considerado una falta a la normativa interna, y podrá ser sancionado de acuerdo a la gravedad de la falta incurrida, previa evaluación de la intencionalidad, impacto y daño que cause a UDP, de acuerdo a lo establecido en el Reglamento Interno de Orden Higiene y Seguridad.

7. Definiciones preliminares y roles

Información: La información es la interpretación que se da a un conjunto de datos, pudiendo residir ésta en medios físicos o en el conocimiento de las personas. En el caso de la presente política, se entenderá como información toda aquella proveniente de datos relacionados con los procesos que involucran la actividad asociada a la universidad y sus relacionadas, así como la proporcionada tanto por los/as usuarios/as internos como los externos, en el contexto del ejercicio de sus funciones y del cumplimiento de sus obligaciones.

Seguridad de la Información: Nivel de confianza que la organización desea tener de su capacidad para preservar la autenticidad, confidencialidad, integridad y disponibilidad de la información. Tiene como objetivo proteger el recurso información de una amplia gama de amenazas, con el fin de asegurar la continuidad de los procesos dentro de la universidad, minimizar el daño y, cumplir su misión y objetivos estratégicos.

Activo de Información: De acuerdo con la norma ISO 27001, se define como aquel recurso que una organización valora por la información que maneja, y por lo tanto debe proteger. Para el caso de la universidad, los activos de información se categorizan en: información propiamente, procesos relevantes, sistemas relevantes, entre otros activos, los cuales se detallan en la Política de Gestión de Activos de Información (PO.08.00.00).

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de prácticas y procesos orientados a garantizar y preservar la autenticidad, confidencialidad, integridad y disponibilidad de la información.

Autenticidad: Aseguramiento de la validez de la información en tiempo, forma, distribución y autoría (validando al emisor para evitar suplantación de identidades, entre otras).

Confidencialidad: Aseguramiento que la información es accesible sólo para las personas autorizadas para ello.

Integridad: Salvaguarda en la exactitud y totalidad de la información en su procesamiento, transmisión y almacenamiento.

Disponibilidad: Aseguramiento que los/as usuarios/as autorizados tengan acceso a la información y a los activos asociados cuando estos sean requeridos.

Personal: Toda persona a la cual se le concede autorización para acceder a la información y a los sistemas de la universidad y sus relacionadas. El personal puede ser interno o externo a la organización.

Contraloría: Unidad que fiscalizará el correcto cumplimiento de lo expresado en esta política a través de revisiones sorpresivas o programadas.

Comité de Seguridad y Riesgo: Órgano encargado de supervisar la implementación del sistema de gestión de seguridad de la información SGSI, garantizando su funcionamiento, eficacia y mejora continua.
(*) Se ha establecido la formalización del Comité de Seguridad y Riesgo durante el Q1 del año 2021.

Director/a General de Sistemas de Información: Persona responsable del área de Sistemas y encargada de administrar los recursos asociados a los activos de información.

Oficial de Seguridad de la Información: Persona responsable de la definición, diseño, implementación, difusión, capacitación y supervisión de las medidas asociadas a la seguridad de la información.

Propietario/a de la Información: Es la persona responsable del proceso que contiene alguna información relevante para la organización. Por ende, es la encargada de definir lineamientos tales como los accesos permitidos, la tolerancia ante determinados riesgos y la clasificación de criticidad de la información a su cargo. así como también, es el/la responsable de asegurar que los planes de acción y controles establecidos para los activos de información se implementen y operen de manera efectiva.

8. Reglas de la política global de seguridad de la información

8.1 Generalidades.

a) La universidad y sus relacionadas reconocen la información como un activo esencial para la organización, por lo que debe ser administrada con el mismo rigor que el resto de los activos de la institución, entendiéndose que la información puede estar contenida en medios magnéticos o en papel, almacenada electrónicamente, transmitida por medios digitales, mostrada en videos o transmitida en forma verbal.

b) La información debe ser protegida por todo el personal de manera adecuada a su sensibilidad y valor, resguardando su confidencialidad, integridad y disponibilidad.

c) La información de la universidad y sus relacionadas no debe quedar disponible a personas o entidades externas, salvo en las situaciones y formas expresamente establecidas en los acuerdos vigentes y con controles que garanticen la protección de la información.

d) La seguridad de la información de la universidad y sus relacionadas y de los bienes asociados al manejo de esa información, es responsabilidad de todas y cada una de las personas que la integran, independiente del cargo que desempeñen.

e) Cada funcionario/a de la universidad y sus relacionadas debe acceder responsablemente a la mínima cantidad de información que le sea necesaria para cumplir sus funciones, y tiene la obligación de notificar cualquier actividad o situación que contravenga estos lineamientos.

f) De esta política global, se desprenden las restantes políticas de seguridad de la información, que constituyen la definición fundamental de los planteamientos de seguridad de la universidad y sus relacionadas en materias específicas, haciendo hincapié en el rol que deben asumir todos los funcionarios para lograr el resguardo de la información y los recursos asociados.

g) El Comité de Seguridad y Riesgo tiene la autoridad y responsabilidad para decidir y velar por la existencia de las medidas de seguridad destinadas a proteger y preservar los activos de información de la organización. La implantación y efectiva aplicación de las medidas de seguridad que se

definan corresponderá a las áreas administrativas y académicas de la universidad y sus relacionadas, las que serán coordinadas en su acción por el Oficial de Seguridad de la Información. De acuerdo con la Resolución N° 020/2018, este comité estará conformado por:

- Director/a General de Sistemas de la Información.
- Director/a de Recursos Humanos.
- Director/a General de Finanzas y Presupuestos.
- Representante de la Dirección de Administración Académica.
- Dirección Registro y Certificación.
- Dirección Jurídica.
- Dirección de Mejoramiento Continuo.
- Dirección de Comunicaciones.
- Oficial de Seguridad de la Información.

h) La universidad y sus relacionadas impone un deber a todo aquel que preste servicios a cualquier título para la organización, de mantener en estricto secreto toda la información y cualquier otro antecedente que conozca en el ejercicio de su cargo, y se relacione directa o indirectamente con sus funciones y actividades.

i) Esta política y sus definiciones han sido aprobadas por UDP y difundidas al interior de toda la organización, por tanto, deben ser cumplidas por todos/as los/as funcionarios/as de la universidad y sus relacionadas y por quienes presten servicios en ella. Todos ellos, tendrán la obligación de informar los incidentes que atenten contra la seguridad de información y de informar situaciones que vayan en contra de lo descrito en esta política y sus procedimientos relacionados. Dichos reportes de incidentes deberán ser comunicados al Oficial de Seguridad de la Información, a través de un correo electrónico dirigido a "Incidente.Seguridad@udp.cl".

j) Las disposiciones relacionadas con las normas y políticas referidas a la seguridad de la información serán debidamente controladas en su cumplimiento por las áreas definidas al interior de la organización.

8.2 Responsabilidades.

El detalle de la estructura organizacional responsable de la seguridad de la información en nuestra universidad se documenta en: “PO.06.00.00 - Política de Organización de Seguridad de la Información”.

8.3 Atributos de la información que se deben proteger.

Es responsabilidad de la universidad y sus relacionadas resguardar los siguientes atributos de la información:

a) Integridad: Se debe garantizar que todos los datos, información y transacciones se encuentren libres de errores y/o irregularidades de cualquier índole.

b) Disponibilidad: Se debe garantizar que la información esté disponible cuando un usuario, entidad o proceso autorizado lo requiera. Además, se debe garantizar que las tareas críticas no tengan interrupciones que pongan en riesgo la continuidad de las operaciones.

c) Confidencialidad: Se debe garantizar que toda información (física y digital) y sus medios de procesamiento, transmisión 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.

8.4 Nomenclatura de documentos.

La nomenclatura de los documentos relativos a la administración y gestión de la seguridad de la información se compone de los siguientes campos que conforman el código de identificación del documento:

Tipo de documento (a.)	“.“	Dominio de Alcance (b.)	“.“	Objetivo de la materia normada asociada al Dominio (c.)	“.“	ID del documento (d.)	“-“	Título (e.)

a) Tipo de documento (dos caracteres):

- PO, Política.
- NO, Norma.
- PR, Procedimiento.

UNIVERSIDAD DIEGO PORTALES DIRECCIÓN JURIDICA

- FO, Formulario.
- AN, Anexo.

b) Capítulo o alcance de acuerdo con el ámbito según las recomendaciones de la norma ISO 27001:2013:

- 05 - Políticas de Seguridad de la Información.
- 06 - Aspectos Organizativos de la Seguridad de la Información.
- 07 - Seguridad ligada a los Recursos Humanos.
- 08 - Gestión de Activos de Información.
- 09 - Control de Accesos.
- 10 - Criptografía de la Información.
- 11 - Seguridad Física y Ambiental.
- 12 - Seguridad de las Operaciones.
- 13 - Seguridad de las Comunicaciones.
- 14 - Adquisición, Desarrollo y Mantenimiento de los Sistemas.
- 15 - Relación con los Proveedores.
- 16 - Gestión de Incidentes en la Seguridad de la Información.
- 17 - Gestión de la Continuidad del Negocio.
- 18 - Cumplimiento.

c) Objetivo de la materia normada: asociada al capítulo de la norma ISO 27001:2013.

d) N° de identificación del documento (dos dígitos): correlativo del documento dentro de un mismo Capítulo-Objetivo.

e) Título (libre): título descriptivo de documento.

Ejemplos de Nomenclatura:

- PO.09.02.00 – Política de Seguridad Gestión de Cuentas de Usuarios.
- PO.12.03.00 – Política de Respaldos Generales.

9. Revisión de la Política

El/la Oficial de Seguridad de la Información, en conjunto con el Comité de Seguridad y Riesgo, revisará la Política de Seguridad de la Información, al menos, una vez al año después de su fecha de emisión, así como también, será revisada y ajustada en el caso de ocurrir algún cambio significativo, relacionado con:

UNIVERSIDAD DIEGO PORTALES DIRECCIÓN JURÍDICA

- Cambios del entorno y el funcionamiento de la universidad o sus relacionadas (por ejemplo, pandemias o casos excepcionales).
- Cambios relevantes en las condiciones legales.
- Cambios significativos en un activo de información (por ejemplo, sustitución del sistema Core).

10. Anexo

a) El listado de las políticas de seguridad se encuentra definidas y formalizadas en la Intranet Corporativa: (**https://contraloria.udp.cl/politicas-y-procedimientos/).**

PO.05.00.00 - Política Global de Seguridad de la Información.
PO.06.00.00 - Política de Organización de Seguridad de la Información.
PO.06.02.00 - Política de Seguridad en las Conexiones Remotas.
PO.08.00.00 - Política de Gestión de Activos de Información.
PO.08.02.00 - Política de Seguridad en Gestión Documental.
PO.09.02.00 - Política de Seguridad Gestión de Cuentas de Usuarios.
PO.10.00.00 - Política de Controles Criptográficos.
PO.11.01.00 - Política para el Control del Acceso Físico.
PO.12.01.00 - Política Desarrollo y Mantenimiento de Sistemas.
PO.12.03.00 - Política de Respaldos Generales.
PO.12.04.00 - Política para el Monitoreo de Servidores y Dispositivos de Red.
PO.12.06.00 - Política de Protección y Configuración de Servidores.
PO.13.01.00 - Política para el Uso de la Red e Internet.
PO.14.01.01 - Política de Administración de Dominios.
PO.14.02.00 - Política de Seguridad para la Mantención y Adquisición de Sistemas.
PO.16.00.00 - Política de Gestión de Incidentes de Seguridad de la Información.
PO.17.00.00 - Política de Gestión de la Continuidad de Negocios.
PO.18.00.00 - Política de Seguridad sobre el Cumplimiento Legal.