

FUNDACIÓN INSTITUTO PROFESIONAL DUOC UC
RESOLUCIÓN RECTORÍA N°11/2024
APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

VISTOS Y CONSIDERANDOS:

- 1° Que, la Fundación Instituto Profesional Duoc UC es una Institución de Educación Superior, constituida legalmente como una fundación privada sin fines de lucro y que, por tanto, se encuentra sometida a la normativa vigente aplicable a este tipo de personas jurídicas como asimismo a toda la normativa de educación superior vigente a esta fecha.
- 2° Que, conforme a las facultades otorgadas por la letra f) del artículo 5 del Reglamento General vigente y demás aplicables.

RESUELVO:

PRIMERO: Apruébese la “*Política General de Seguridad de la Información*”, la que se adjunta a continuación de esta resolución.

SEGUNDO: La Política General de Seguridad de la Información antes aprobada entrará en vigencia a contar de esta fecha.

Comuníquese, publíquese y regístrese.

Santiago, junio 18 de 2024.



JOSE HUMBERTO SEPULVEDA CAVIEDES
SECRETARIO GENERAL


CARLOS DÍAZ VERGARA
RECTOR


PEF/csm



POG-SI-01 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN


	Política general de seguridad de la información	Código	POG-SI-01
		Versión №	1 .0
		Fecha de edición	18.06.2024
	Sistema de gestión de seguridad de la información	Vigencia	Indefinida con revisión periódica.
		Página	1 de 14
		Confidencialidad	Interna

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

	Política general de seguridad de la información	Código	POG-SI-01
		Versión Nº	1 .0
		Fecha de edición	18.06.2024
	Sistema de gestión de seguridad de la información	Vigencia	Indefinida con revisión periódica.
		Página	2 de 14
		Confidencialidad	Interna

Contenido

CONTEXTO	3
1. OBJETIVO.	3
2. ALCANCE.	4
3. DEFINICIONES.	4
4. PRINCIPIOS.	5
5. REQUISITO O CONTROL DE LA NORMA ISO AL QUE RESPONDE.	7
6. RIESGOS ABORDADOS.	7
7. ORGANIZACIÓN DE LA SEGURIDAD.	8
8. DEL MARCO NORMATIVO INTERNO DE SEGURIDAD DE LA INFORMACIÓN.	12
9. AUDITORIA INTERNA Y CUMPLIMIENTO.	13

	Política general de seguridad de la información	Código	POG-SI-01
		Versión Nº	1 .0
		Fecha de edición	18.06.2024
	Sistema de gestión de seguridad de la información	Vigencia	Indefinida con revisión periódica.
		Página	3 de 14
		Confidencialidad	Interna

CONTEXTO


En el compromiso constante con la excelencia académica y la formación integral de nuestros estudiantes, Duoc UC, se enorgullece en presentar su Política General de Seguridad de la Información (en adelante la “**Política**”). Guiados por los valores fundamentales de una institución católica, esta política busca salvaguardar la confidencialidad, integridad y disponibilidad de la información, reconociendo la importancia crítica que los recursos digitales tienen en la consecución de nuestros objetivos institucionales. A través de esta iniciativa, aspiramos a fomentar un entorno seguro, fortaleciendo la protección de información y datos sensibles y promoviendo prácticas responsables en el uso de la tecnología, en consonancia con nuestra misión de formar profesionales éticos y competentes en un mundo cada vez más interconectado.

A medida que avanza la transformación digital y la interacción y dependencia de las personas e instituciones con la tecnología, crece la superficie de riesgos a que nos vemos expuestos. Así, vemos, por ejemplo, como actores maliciosos o fenómenos de la naturaleza pueden impactar severamente en la vida de las personas y en procesos de las instituciones y de los Estados. Hoy vemos que los métodos de propagación de ransomware, phishing, cryptojacking, entre otros se han sofisticado y son cada día más recurrentes. Por otro lado, el Estado ha impulsado la actualización de marcos legales para salvaguardar las crecientes necesidades de privacidad y seguridad de los ciudadanos que también nos obliga a adaptarnos.

En este nuevo escenario, se hace indispensable contar con estrategias de seguridad cibernética cada vez más robustas que den respuestas a los marcos legales y a protección de la seguridad de la información que nuestros usuarios nos demandan.

1. OBJETIVO.

Esta Política tiene como objetivo establecer los criterios y directrices generales sobre la gestión de seguridad de la información de *Duoc UC*, en los cuales se basan las demás políticas

	Política general de seguridad de la información	Código	POG-SI-01
		Versión Nº	1 .0
		Fecha de edición	18.06.2024
	Sistema de gestión de seguridad de la información	Vigencia	Indefinida con revisión periódica.
		Página	4 de 14
		Confidencialidad	Interna

específicas, normas y procedimientos. Esto incluye los principios básicos de la seguridad de la Información en *Duoc UC*, en concordancia con las estrategias y objetivos de negocio.

Igualmente, esta Política busca traspasar los principios de la seguridad de la información a las partes interesadas de la Institución, para proyectar a *Duoc UC* como promotora del cuidado de la información, de la ciberseguridad y de la privacidad de los datos.

2. ALCANCE.


La Política aplica a todos los activos de información de Duoc UC, cualquiera sea el formato y el soporte, así como los procesos que lo apoyan.

El Instituto Profesional DUOC UC, en adelante Duoc UC, declara que la información de la Institución es un activo fundamental para la toma de decisiones eficientes y, por consiguiente, para el logro de los objetivos estratégicos, por lo que su protección es primordial.

Es por lo que la gestión de seguridad de la información en Duoc UC se lleva a cabo como un proceso continuo, destinado a proteger los activos de información contra amenazas internas y externas que pudiesen tener un impacto económico, legal y/o reputacional para la Institución. Esto se logra a través de la adopción de los requisitos de la seguridad de la información, ciberseguridad y protección de la privacidad de la norma ISO/IEC 27001: 2022, estableciendo con esto un sistema de gestión de seguridad de la información conforme con un estándar reconocido y mundialmente aceptado.

3. DEFINICIONES.

Activo de información: Son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la Institución, en la que se distinguen tres niveles:

	Política general de seguridad de la información	Código	POG-SI-01
		Versión Nº	1 .0
		Fecha de edición	18.06.2024
	Sistema de gestión de seguridad de la información	Vigencia	Indefinida con revisión periódica.
		Página	5 de 14
		Confidencialidad	Interna

- La información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.)
- Los equipos/sistemas/infraestructura que soportan esta información.
- Las personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.

Confidencialidad: Propiedad que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad que consiste en que la información está disponible y es utilizable cuando es requerida por un individuo, entidad o proceso autorizado.

Información: Se refiere a un conjunto organizado de datos que los colaboradores de la organización generan, obtienen, transforman o controlan.

Integridad: Propiedad que consiste en que la información no ha sido modificada o destruida sin autorización, asegurando que los datos se mantengan completos y exactos durante su creación, transmisión y almacenamiento.

Requisito: Necesidad o expectativa establecida, generalmente implícita u obligatoria.


Riesgo: Efecto de la incertidumbre sobre la consecución de los objetivos.

Seguridad de la información: Preservación de la integridad, disponibilidad y confidencialidad de la información.

Sistema de gestión: Actividades mediante las que la organización identifica sus objetivos, determina y gestiona los procesos y recursos requeridos para lograr los resultados deseados.

4. PRINCIPIOS.

Los principios del sistema de gestión de seguridad de la información de Duoc UC son:

	Política general de seguridad de la información	Código	POG-SI-01
		Versión Nº	1 .0
		Fecha de edición	18.06.2024
	Sistema de gestión de seguridad de la información	Vigencia	Indefinida con revisión periódica.
		Página	6 de 14
		Confidencialidad	Interna

Principio de disponibilidad, confidencialidad e integridad.


- Mantener los niveles de disponibilidad, confidencialidad e integridad requeridos para los activos de información de la Institución, inclusive si son alojados y administrados por terceros en dependencias de un proveedor de tecnología; mediante la implementación de controles de seguridad de la información eficaces, acordes a los requisitos legales y contractuales aplicables, y a la gestión de riesgos llevada a cabo por los procesos de la Institución, y que finalmente quedarán reflejados en nuestra Declaración de Aplicabilidad.

Principio de corresponsabilidad o accountability.

- Cumplir y hacer cumplir los compromisos de seguridad de la información en los tiempos establecidos, sobre todo aquellos referidos a la ejecución de los controles de seguridad de la información, mediante el establecimiento de roles que hagan seguimiento y medición a lo propio, con la suficiente autoridad para garantizar la seguridad de la información en la Institución.
- En todo momento, dar cumplimiento a los requisitos de seguridad de la información establecidos en leyes, regulaciones y normativas aplicables a los servicios que Duoc UC proporciona a sus usuarios, asegurando lo propio mediante el establecimiento de procesos que hagan seguimiento y medición a dicho cumplimiento.
- Mejorar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de seguridad de la información, con el objeto de dar valor a la Institución como un todo.

Principio de coordinación y colaboración entre áreas.

Los colaboradores, proveedores, personal externo y todos aquellos que tengan relación directa o indirecta con el tratamiento, almacenamiento, manipulación, transmisión o resguardo de los activos de información de *Duoc UC*, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados.

	Política general de seguridad de la información	Código	POG-SI-01
		Versión Nº	1 .0
		Fecha de edición	18.06.2024
	Sistema de gestión de seguridad de la información	Vigencia	Indefinida con revisión periódica.
		Página	7 de 14
		Confidencialidad	Interna

Principio de Constitucionalidad y Legislación

Esta Política deberá mantener un lineamiento acorde a las directrices definidas por la organización, siempre considerando el marco constitucional y legislativo vigente en nuestro país, particularmente lo referido a los derechos y libertades de las personas y otras leyes aplicables al campo de la información, de los datos personales y la tecnología.

Relaciones con Proveedores


Con el fin de dar continuidad de forma segura a la entrega de los servicios o productos prestados por proveedores externos, específicamente aquellos asociados al tratamiento de información, es fundamental garantizar que el proveedor cuente al menos con el mismo estándar de mecanismos y controles de seguridad definidos por la organización; en consecuencia, los proveedores deberán estar en conocimiento de la Política de Seguridad de la Información de Duoc UC, cumpliendo para tal efecto todas las obligaciones contractuales que les relacionen con Duoc UC.

5. REQUISITO O CONTROL DE LA NORMA ISO AL QUE RESPONDE.

Esta Política de Duoc UC se encuentra soportada por otras políticas, normas y procedimientos específicos, las cuales se fundamentan en el estándar internacional norma ISO/IEC 27001:2022, que tienen como objeto el implementar, mantener y llevar a cabo las mejores prácticas en lo que se refiere a seguridad de la información y permanente mejora continua.

6. RIESGOS ABORDADOS.

Los indicados en la Matriz de riesgos del SGI de DUOC UC.

	Política general de seguridad de la información	Código	POG-SI-01
		Versión Nº	1 .0
		Fecha de edición	18.06.2024
	Sistema de gestión de seguridad de la información	Vigencia	Indefinida con revisión periódica.
		Página	8 de 14
		Confidencialidad	Interna

7. ORGANIZACIÓN DE LA SEGURIDAD.

Esta Política de Duoc UC, es un documento redactado por el Comité Estratégico de Seguridad de la Información y aprobado por el Consejo Superior de Duoc UC.

Todos los colaboradores de Duoc UC son responsables del cumplimiento de esta Política. El Rector, vicerrectores, directivos y todas las jefaturas, son responsables de asegurar que el personal de Duoc UC y de empresas externas que tengan acceso a los activos de la información cumplan con esta Política.


El sistema de gestión de seguridad de la información implementado en la Dirección General de Servicios Digitales de Duoc UC debe cumplir con lo establecido en esta Política, siendo la base para el establecimiento de políticas específicas y otros lineamientos.

Oficial de Seguridad de la Información:

El Oficial de Seguridad de la Información es el responsable de mantener un nivel adecuado de protección de la información de Duoc UC, asegurando la integridad, disponibilidad y confidencialidad de la información de la Institución.

El Oficial de Seguridad de la Información tiene como responsabilidades:

- Asegurar que esta Política cumple con los requisitos de la norma sobre sistemas de gestión de seguridad de la información.
- Asegurar una adecuada comunicación de la política general de los sistemas de gestión.
- Planificar, desarrollar, y hacer seguimiento a las políticas, normas y procedimientos de seguridad de la información de la Institución.

	Política general de seguridad de la información	Código	POG-SI-01
		Versión Nº	1 .0
		Fecha de edición	18.06.2024
	Sistema de gestión de seguridad de la información	Vigencia	Indefinida con revisión periódica.
		Página	9 de 14
		Confidencialidad	Interna


- Asesorar en forma permanente a las distintas áreas de la Institución en temas referentes a seguridad de la información, y conducir el correcto cumplimiento de los estándares de seguridad definidos.
- Coordinar las evaluaciones de riesgos de seguridad de la información, planificar la implementación de los controles de seguridad de la información con los dueños de riesgos y documentar la aplicabilidad de estos controles en las declaraciones correspondientes.
- Promover iniciativas y proyectos que permitan resguardar la información de la Institución.
- Gestionar incidentes de seguridad de la información y la continuidad de la seguridad de la información.
- Promover una cultura de seguridad de la información en la Institución.
- Supervisar la implementación y el cumplimiento de esta Política.
- Las demás funciones descritas en su descripción de cargo.

Comité estratégico de seguridad de la información:

El Comité Estratégico de Seguridad de la Información (en adelante el “**Comité**”) está compuesto por:

- Rector
- Director de Cumplimiento
- Director de Contraloría
- 1 Director de Sede
- Directora General de Servicios Digitales
- Director de Servicios Tecnológicos
- Oficial de Seguridad de la Información

El Comité sesionará en forma ordinaria y extraordinaria. Las sesiones ordinarias se fijarán de forma anual. Las sesiones extraordinarias serán convocadas por el Oficial de Seguridad

	Política general de seguridad de la información	Código	POG-SI-01
		Versión Nº	1 .0
		Fecha de edición	18.06.2024
	Sistema de gestión de seguridad de la información	Vigencia	Indefinida con revisión periódica.
		Página	10 de 14
		Confidencialidad	Interna

de la Información, cada vez que se requiera y cuando afecte a la continuidad de los procesos críticos de la Institución.

El Comité tiene como responsabilidades:


- Asegurar que se defina la política general de seguridad de la información y que ésta sea compatible con la dirección estratégica de la organización.
- Proponer al Consejo Directivo de la organización la política general de seguridad de la información.
- Definir los lineamientos para la gestión de seguridad de la información, a través del establecimiento de políticas generales, y asignar los recursos que sean necesarios para la implementación de estos.
- Revisar y aprobar las políticas específicas y normas de seguridad de la información que sea necesario generar o modificar, que apoye a la adecuada gestión de la seguridad de la información.
- Velar que se gestionen los riesgos a los cuales se encuentran expuestos los activos de información de la Institución.
- Aprobar iniciativas y proyectos para mejorar la seguridad de los activos de información.
- El Comité determinará y aprobará la asignación de recursos adicionales a los ya presupuestados, cada vez que sea pertinente.

Consejo Directivo de DUOC UC:

El Consejo Directivo de Duoc UC (el “**Consejo**”) tiene como responsabilidades:

- Aprobar la política general de seguridad de la información, promover su permanente difusión y adopción por parte de la comunidad educativa, propiciando su revisión y actualización al menos cada dos años.

Propietarios o responsables de Activos de Información:

	Política general de seguridad de la información	Código	POG-SI-01
		Versión Nº	1 .0
		Fecha de edición	18.06.2024
	Sistema de gestión de seguridad de la información	Vigencia	Indefinida con revisión periódica.
		Página	11 de 14
		Confidencialidad	Interna

El propietario (también denominado responsable) de un activo de información es un colaborador (o una entidad) que la organización ha asignado como responsable de gestionar su ciclo de vida completo, esto en concordancia con los procesos de gestión de Riesgos.

El propietario de activos de información tiene como responsabilidades:

- Asegurar que los activos que se le han asignado estén protegidos y seguros.
- Asegurar que los activos son inventariados.
- Asegurar que los activos son clasificados y protegidos adecuadamente (gestiona el riesgo).
- Garantizar el manejo adecuado cuando el activo es eliminado o destruido.


Colaboradores de la organización:

Los colaboradores de la organización tienen como responsabilidades:

- Dar cumplimiento a la política general de seguridad de la información.

Duoc UC hará responsable al colaborador de las consecuencias del incumplimiento de las reglas establecidas en esta Política, de acuerdo con el proceso disciplinario definido por la organización.

A continuación, se presenta la interrelación del **Comité Estratégico de Seguridad de la Información** con la comunidad *Duoc UC*:


	Política general de seguridad de la información	Código	POG-SI-01
		Versión Nº	1 .0
		Fecha de edición	18.06.2024
	Sistema de gestión de seguridad de la información	Vigencia	Indefinida con revisión periódica.
		Página	12 de 14
		Confidencialidad	Interna



8. DEL MARCO NORMATIVO INTERNO DE SEGURIDAD DE LA INFORMACIÓN.

La documentación interna de la Seguridad de la Información de Duoc UC se encuentra agrupada en:

- **Políticas:** Documentos que establecen las necesidades y requisitos de protección en el ámbito de seguridad de la información, y es la guía para la creación de otros tipos de documentos más detallados.
- **Normas:** Documentos que establecen los requisitos que sustentan una política. Define específicamente lo que se debe proteger y en qué condiciones.
- **Procedimientos:** Documentos que determinan las acciones o tareas a realizar en el desempeño de un proceso relacionado con la seguridad de la información y las personas o grupos responsables de su ejecución.

	Política general de seguridad de la información	Código	POG-SI-01
		Versión Nº	1 .0
		Fecha de edición	18.06.2024
	Sistema de gestión de seguridad de la información	Vigencia	Indefinida con revisión periódica.
		Página	13 de 14
		Confidencialidad	Interna

Esta Política es la base para la generación de políticas específicas relativas a la seguridad de la información dentro de Duoc UC. Por tanto, la presente Política establece los lineamientos generales de seguridad de la información en Duoc UC.

9. AUDITORIA INTERNA Y CUMPLIMIENTO.

La Dirección de Contraloría y la Dirección de Cumplimiento podrán ejecutar procesos sistemáticos, independiente y documentados para obtener evidencias objetivas con el fin de determinar el grado de cumplimiento de lo establecido en la Política.

10. VIGENCIA.

Esta Política entrará en vigencia una vez aprobada por el Consejo Directivo de Duoc UC y comunicada a la comunidad institucional mediante la dictación de la correspondiente resolución de Rectoría.