FUNDACIÓN INSTITUTO PROFESIONAL DUOC UC
RESOLUCIÓN RECTORÍA N°18/2024

APRUEBA POLÍTICA DE CLASIFICACIÓN DE DATOS E INFORMACIÓN

VISTOS

i. Constitución Política de la República de Chile, artículo 19 N°4.
ii. Ley 19.628 sobre Protección de la Vida Privada.
iii. Ley 21.459, delitos informáticos establece normas sobre delitos informáticos, deroga la ley N°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.
iv. Ley 20.393 Ley de Responsabilidad Penal de las Personas Jurídicas.
v. Ley N°19.496, establece normas sobre protección de los derechos de los consumidores.
vi. Ley N°19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
vii. Código de Ética y Conducta de la Fundación Instituto Profesional Duoc UC.
viii. Reglamento Interno de Orden, Higiene y Seguridad de la Fundación Instituto Profesional Duoc UC.
ix. Política de Gobierno de Datos, Duoc UC, Resolución Rectoría 09/2023.

CONSIDERANDO

i. 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 la fecha.

ii. Que, en el ejercicio del quehacer institucional, la Fundación Instituto Profesional Duoc UC a través de la Dirección de Gobierno de Datos y Análisis Institucional y la Dirección General de Servicios Digitales ha surgido la necesidad de elaboración de una Política de Clasificación de Datos e información con ocasión de las nuevas regulaciones legales y reglamentarias. Asimismo, la presente política refuerza e impulsa a la mejora en el manejo y tratamiento de información, de manera de mejorar la gestión interna, utilizando de la manera más eficaz el dato y la información como una herramienta estratégica clave para lograr el mejoramiento de la gestión institucional con miras al cumplimiento del fin educacional en todos sus niveles y grados, con estricta sujeción a la legislación vigente.

iii. Que, la presente política tiene por objeto, entre otros, contribuir a partir del establecimiento de un sistema de clasificación al correcto resguardo y confidencialidad a que todo colaborador/a está obligado a cumplir en Duoc UC en el manejo de datos e información y su tratamiento, ya sea por el cargo y/o función que desempeña al interior de la institución, como, asimismo, por constituir una regla general en materia de protección de datos e información a que todo integrante de la comunidad educativa está obligado a ceñirse.

iv. Que, a mayor abundamiento, los colaboradores/as designados al efecto para obtener, manejar y administrar información que contenga información y datos deben cumplir necesariamente los resguardos exigidos por la legislación que regula la materia sobre el uso y reserva de los mismos.

v. Que, en razón de lo anteriormente señalado y conforme a las facultades previstas en las letras c, f y g del artículo 5° del reglamento general vigente aprobado por Decreto de Rectoría N°01/2024 de fecha 22 enero de 2024, es procedente la dictación de la presente resolución que aprueba la Política de Clasificación de Datos e Información de la Fundación Instituto Profesional Duoc UC.

RESUELVO

APRUÉBASE la Política de Clasificación de Datos e Información de la Fundación Instituto Profesional Duoc, que forma parte integrante de esta resolución.

Comuníquese, publíquese y regístrese.

Santiago, octubre 22 de 2024.

CARLOS DÍAZ VERGARA
RECTOR

VL/RY/GGP/XS/PE/JSC

POLÍTICA DE CLASIFICACIÓN DE DATOS E INFORMACIÓN DUOC UC

REVISIONES Y APROBACIONES

Nombre	Rol	Versión	Fecha de Creación/Modificación/revisión
Victor León	Oficial de Seguridad, DGSD	1	30/08/2023 Crea
Ghia Gajardo Pineda	Directora de Gobierno de Datos y Análisis Institucional	1	10/06/2024 Modifica
Ximena Sibils	Directora General de Servicios Digitales	1	08/10/2024 Modifica y Aprueba
Ghia Gajardo Pineda	Directora de Gobierno de Datos y Análisis Institucional	1	10/10/2024 Aprueba
Pilar Estay	Directora Jurídica	1	16/10/2024 Aprueba
José Humberto Sepúlveda	Director de Cumplimiento y Secretario General	1	16/10/2024 Aprueba

ÍNDICE

1. CONTEXTO

En el contexto de la implementación del Gobierno o Gobernanza de Datos de Duoc UC definido en la Política de Gobierno de Datos Institucional, y considerando la importancia de los datos e información[1] para la gestión de la excelencia y calidad en la toma de decisiones, es que se reconoce a los datos e información como activos de información que deben ser protegidos. Lo anterior, con estricta sujeción a la normativa vigente, en especial aquella que resguarda la propiedad intelectual, industrial y secretos comerciales de Duoc UC y terceros, así como la protección de los datos personales de las personas, velando por el constante resguardo y el respeto al pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades reconocidas por el ordenamiento jurídico de manera eficiente, oportuna y eficaz.

Considerando lo anterior, el Gobierno de Datos establece un marco, junto con mecanismos e instancias de decisiones que, al ser adoptados, reducen riesgos asociados al uso de los datos. Además, permite a la organización aprovecharlos de manera estratégica para dar cuenta del cumplimiento de sus objetivos institucionales con estricta sujeción a la normativa que regula la protección de los mismos, al establecer los lineamientos para su uso y alertas en caso indebidos del uso.

Para alcanzar el propósito institucional, Duoc UC ha definido la necesidad de establecer una clasificación de los datos e información que le permita implementar los principios de seguridad, confidencialidad y privacidad (ver punto 3 de la Política de Gobierno de Datos) garantizando, asimismo, el cumplimiento de los Derechos de los Titulares de los datos (ver punto 1.2 Política de Gobierno de datos)

2. ALCANCE

Esta política es aplicable a todos los datos e información tratada por la Institución, independientemente de las fuentes, formato o soporte, en todo el ciclo de vida del dato (ver punto 1.1 de la Política de Gobierno de Datos) e involucra a toda la comunidad educativa que forma parte de la Institución con sus respectivas Direcciones tanto académicas y administrativas, y a todas sus áreas y procedimientos, en los niveles, estratégicos, tácticos y operativos.

Proveedores o Terceros:

[1] Los datos son la representación de hechos como texto, números, gráficos, imágenes, sonido o vídeo. Técnicamente, datos es el plural de la palabra proveniente del latín datum, que significa "un hecho". Los hechos son capturados, almacenados y se expresan como datos. La información son datos en un contexto. (Fuente: DAMA)

Los proveedores o terceros, y específicamente aquellos asociados al tratamiento, administración, y manejo de datos e información de Duoc UC, sus administrativos y estudiantes deberán estar en conocimiento de esta Política y garantizar su cumplimiento.

3. OBJETIVO

El Objetivo es establecer un sistema de clasificación de datos e información en la institución, basado en los principios definidos en Gobierno de Datos, en especial a lo referido a la integridad y estandarización, así como la seguridad, confidencialidad y privacidad, estableciendo lineamentos de etiquetado, manipulación y uso de éstos de acuerdo con la clasificación definida.

4. DEFINICIONES

Activo de información: Corresponde a todos los datos y análisis de éstos que la institución produce, emite, captura o recupera, almacena, comunica, usa y visualiza para su gestión. Dentro de estos se distinguen tres tipos:

- Datos e información propiamente tal, en sus múltiples formatos (Papel, digital texto, imagen, audio, video, etc.)
- Equipos/sistemas/infraestructura y múltiples fuentes (sistemas, plataformas, aplicativos, encuestas, sondeos, datos públicos, etc.) que soportan los datos e información.
- Personas que acceden, visualizan y utilizan datos e información.

Dato: Representación de hechos como texto, números, gráficos, imágenes, sonido o vídeo. Técnicamente, datos es el plural de la palabra proveniente del latín datum, que significa “un hecho”. Los hechos son capturados, almacenados y se expresan como datos.

Dato personal: cualquier información vinculada o referida a una persona natural identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante uno o más identificadores, tales como el nombre, el número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
Para determinar si una persona es identificable deberán considerarse todos los medios y factores objetivos que razonablemente se podrían usar para dicha identificación en el momento del tratamiento

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

Información documentada: Información que una organización tiene que controlar y mantener, y el medio que la contiene.

Documento: Información y su medio de soporte.

Tratamiento de datos: Cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, procesar, almacenar,

comunicar, transmitir o utilizar de cualquier forma Datos Personales o conjuntos de Datos Personales.

Titular de Datos Personales o titular: Persona natural, identificada o identificable, a quien conciernen o se refieren los Datos Personales. A mayor abundamiento, el titular de sus datos es toda aquella persona que tiene control sobre sus propios datos personales.

Dueño de dominio o Propietario del Activo: Rol designado por la institución, que tiene la responsabilidad de garantizar que los activos de información que le han sido asignados cuenten con los controles necesarios para asegurar la calidad, la protección y el correcto etiquetado de estos según la clasificación que se indica en esta política.

Responsable de datos: toda persona natural o jurídica, pública o privada, que decide acerca de los fines y medios del tratamiento de datos personales, con independencia de si los datos son tratados directamente por ella o a través de un tercero mandatario o encargado. El responsable debe garantizar estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la naturaleza y clasificación de los datos e información.

Tercero Mandatario o Encargado: Toda persona natural o jurídica, pública o privada, que realiza el acto material de tratamiento de datos e información, por cuenta del responsable de datos.

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

Confidencialidad: Corresponde a la correcta utilización y cuidado de los datos e información al momento de acceder a ellos y en el proceso de toma de decisiones y la gestión, guardando secreto o reserva respecto de la misma y no revelando a individuos, entidades o procesos no autorizados.

Disponibilidad: Se refiere a que los datos e información institucional estén accesibles y disponibles de manera adecuada y controlada cuando sean requeridos.

Integridad: Los datos e información deben tener un alto grado de precisión y exhaustividad asegurando que los datos e información sean fácilmente enlazables y utilizables, es decir, sean susceptibles de ser integrados en todas las unidades funcionales, datas y sistemas electrónicos disponibles, garantizando la existencia de una fuente oficial y valida.

Gestión Responsable: considera garantizar que las áreas involucradas participen activamente en el proceso de creación, gestión y administración de datos e información dentro del marco de las responsabilidades, funciones, perfiles y roles definidos. Lo anterior,

tomando todas las medidas de resguardo internas de los colaboradores que ejercen funciones de alta criticidad en el uso de datos e información institucional.

5. ROLES Y RESPONSABILIDADES

5.1 Director/a de Gobierno de Datos y Análisis Institucional

- Encargado/a de diseñar, proponer y liderar las políticas para la correcta clasificación de datos e información.
- Actuar como facilitador y articulador entre los distintos Dueños de Dominio o Propietarios del activos y áreas para la correcta clasificación de datos e información.
- Velar por el cumplimiento de la política de clasificación de datos e información.
- Asegurar una adecuada comunicación de la política.

5.2 Oficial de Seguridad de la Información - Dirección General de Servicios Digitales

- Asegurar que se establece un esquema de clasificación de la información conforme a lo requerido por el control 5.12 de la ISO/IEC 27001.
- Asegurar que se etiqueta y maneja la información conforme al esquema de clasificación de la información.

- Analizar y verificar el cumplimiento de la política de clasificación de datos e información.
- Colaborar en la adecuada comunicación de la política.

5.3 Dueño de dominio o propietarios de activos

- Definir oportunamente para cada dato o información a su cargo la clasificación que corresponda según la definición de esta política.
- Responsable de identificar los roles y perfiles de acceso a los diversos tipos de datos e información a su cargo, asegurándose de la implementación de la clasificación definida.

5.4 Custodio de datos

- Verificar que la etiqueta de clasificación de la información es incorporada en la información documentada.
- Verificar la implementación de controles de acceso a los datos e información en correspondencia con la clasificación otorgada.

5.5 Directores y subdirectores de Duoc UC

- Revisar la política de clasificación de la información.
- Apoyar en la difusión de la política de clasificación de la información.
- Apoyar y promover la aplicación de la política de clasificación de la información en su equipo.

6. REQUISITO O CONTROL DE LA ISO AL QUE LE RESPONDE

Clasificación de la información (requisito ISO 5.12) y etiquetado de la información

(requisito ISO 5.13)

7. RIESGOS ABORDADOS

Tratamiento inadecuado de la información por falta de clasificación basada en la confidencialidad, integridad, disponibilidad y los requisitos pertinentes de las partes interesadas, cuando estos sean manifiestos.

8. DESARROLLO

Duoc UC reconoce que los datos e información tienen distintos grados de criticidad y sensibilidad, de modo que la clasifica en términos de su valor, y de requisitos legales y contractuales aplicables. La clasificación adoptada permite conocer el grado de protección esperado en el manejo de los datos e información; por lo que a

partir de ésta se pueden reconocer fácilmente las personas que deben acceder a la misma, sus permisos de acceso y cuándo debe estar disponible.

En tal sentido, se distinguen las siguientes categorías:

8.1. Según nivel de Confidencialidad

8.1.1. Información Pública: Datos e Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea colaborador de Duoc UC o no. Corresponde a información que fuere de público conocimiento o conocida mediante publicaciones o cualquier otro medio de comunicación dirigido al público en general o información cuya divulgación o publicación fuere expresamente autorizada por Duoc UC.

8.1.2. Información Interna: Datos e Información que puede ser conocida y utilizada por todos los colaboradores/as de Duoc UC y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la Institución.

8.1.3. Información Confidencial: Datos e Información que sólo puede ser conocida y utilizada por un grupo de colaboradores de Duoc UC, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la Institución o a terceros. Entre los datos e información que caen en esta categoría, pero que no se limitan a esta, corresponde todo dato o información referido a:

Datos Personales: Cualquier dato o información vinculada o referida a una persona natural identificada o identificable a través de medios que puedan ser razonablemente utilizados. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante uno o más identificadores, tales como el nombre, el número de cédula de identidad, domicilio, teléfono, firma manuscrita, correo electrónico, datos bancarios, dirección de IP, entre otros.

8.1.4. Información Reservada: Información y datos que sólo puede ser conocida y utilizada por un grupo muy reducido de colaboradores de Duoc UC, generalmente de la alta dirección, y cuya divulgación o uso no autorizados podría ocasionar pérdidas o impactos graves a la Institución o a terceros. Entre los datos e información que caen en esta categoría, pero que no se limitan a esta, corresponde a todo dato o información referido a:

Dato personal sensible: Aquella información o datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como el origen racial, ideología, afiliación política, creencias o convicciones religiosas o filosóficas, estado de salud físico o psíquico, orientación

sexual, identidad de género e identidad genética y biomédica, entre otros.

8.2 Según nivel de Integridad

8.2.1 Baja: Datos e Información que puede ser modificada por cualquier persona, sea colaborador de Duoc UC o no, pues su pérdida de exactitud y completitud no conlleva un impacto significativo para la entidad o entes externos.

8.2.2 Media: Datos e Información cuya pérdida de exactitud y completitud puede provocar impactos negativos, retrasar operaciones propias o de terceros, o generar pérdida de trazabilidad o visualización para colaboradores/as de la institución, por lo que puede ser modificada por cualquier persona de la organización, siempre que esté otorgado el permiso del Dueño de dominio o propietario del activo.

8.2.3 Alta: Datos e Información cuya pérdida de exactitud y completitud puede provocar un impacto negativo de índole legal, incumpliendo normativo o contractual, provocando multas, demandas o daño en la imagen de la institución frente a terceros, por lo que puede modificarse con permiso del Dueño del Dominio o Propietario del activo, otorgado únicamente a cargos específicos explícitamente identificados.

8.3 Según nivel de Disponibilidad

8.3.1 Baja: Datos e Información cuya no disponibilidad no afecta de manera importante la operación normal de la institución o entes externos relacionados a Duoc UC, no conlleva implicaciones legales, económicas o de deterioro en la imagen de Duoc UC. Su indisponibilidad no puede ser mayor a 48 horas.

8.3.2 Media: Datos e Información cuya no disponibilidad puede afectar la operación normal de la institución o entes externos relacionados a Duoc UC, trayendo consigo implicaciones legales, contractuales, económicas o de deterioro en la imagen de Duoc UC. Su indisponibilidad no puede ser mayor a 24 horas.

8.3.3 Alta: Datos e Información cuya no disponibilidad afecta la continuidad total del servicio educacional afectando la continuidad del negocio, y/o traiga consigo implicaciones de incumplimiento legal, contractual, efectos económicos o de deterioro importante de en la imagen de Duoc UC frente a terceros. Su indisponibilidad no puede ser mayor a 6 horas.

9. ETIQUETADO DE DATOS E INFORMACIÓN

Los Dueños de dominio o propietarios de activos son quienes deben clasificar los datos e información de manera oportuna, esto es, cuando se incorporan sus activos de información en los inventarios correspondientes para su control, y deben comunicar a las áreas involucradas la correcta implementación.

Se debe mantener evidencia de esta clasificación en la etiqueta del activo de datos información, cuando exista, en el mecanismo de registro que defina la Dirección de Gobierno de Datos y Análisis Institucional en conjunto con la Dirección General de Servicios Digitales.

Es responsabilidad del dueño de dominio o propietario del activo preocuparse de clasificar y etiquetar a la brevedad el activo de información y comunicar a las áreas involucradas hasta la correcta implementación.

La revisión de la clasificación de datos e información debe ser periódica, coincidiendo con los tiempos de revisión del Inventario de activos, y coincidiendo con las actualizaciones de datos e información. Esto último se hace pues hay información que pierde su clasificación con el paso del tiempo, por ejemplo, aquella que se convierte en pública por requerimiento o permisos de terceros. Si dentro del periodo de revisión de la clasificación se llegara a detectar algún cambio en los datos o información que supusiera una reclasificación, el Dueño de dominio o propietario del activo es quien debe hacerla oportunamente.

El etiquetado se realiza dependiendo del activo que contiene el dato o información, por ejemplo:

- **Sistemas informáticos:** Deberá ser clasificado mediante una etiqueta de metadatos, si el activo lo permite. Finalmente, el inventario de activos igualmente presenta la clasificación de la información contenida en estos activos.
- **Información documentada en ofimática:** Una etiqueta que presente, de forma inequívoca, si se trata de información confidencial o reservada, pudiendo ser ubicada el encabezado o pie de la página. En el caso de la clasificación que presenten los formularios, será considerada también para los registros que se generen a partir de estos. La información en ofimática también puede presentar su clasificación en una etiqueta de metadatos, que ayuda a prevenir la filtración de datos.
- **Correos electrónicos:** Corresponde a un texto que indica la posibilidad de que éstos contengan información confidencial y serán etiquetados en la firma del correo.
- **Información mantenida en espacios públicos o transmitidos al público** (páginas web, registros públicos, gacetas y boletines), pudiera no presentar la etiqueta de clasificación si se considera redundante.

Será responsabilidad del Dueño de Dominio o propietario del activo, etiquetar los activos físicos y lógicos de acuerdo con el esquema de clasificación establecido en esta política, teniendo el deber de verificar si su etiquetado ocurre y se mantiene vigente y actualizado, esto con el apoyo del Oficial de Seguridad de la Información.

El/la Oficial de Seguridad en acuerdo con el/la Director/a de Gobierno de Datos y Análisis Institucional podrán definir e implementar procedimientos específicos para etiquetar los activos físicos y lógicos, según los consideren necesarios.

10. REGLAS GENERALES PARA EL MANEJO DE LA INFORMACIÓN CLASIFICADA

Para garantizar una manipulación adecuada de la información, se deben tener las siguientes consideraciones:

10.1 Restricciones de acceso: En todos los activos de datos e información, que sean coherentes con la clasificación.

10.2 Mantenimiento de un registro de autorizados al acceso de los activos: En el mecanismo de registro que se defina.

10.3 Mecanismo de traspaso seguro: Se podrán transferir datos e información entre colaboradores mediante el uso de mecanismos definidos por la institución, como, por ejemplo: Carpetas compartidas en one drive institucional, donde se establezca el tipo de acceso – lectura y/o edición y descarga- a usuario/s específicos dentro de la institución en coherencia con la clasificación. (Ver Instructivo para aplicar mecanismo Seguro de Traspaso de Datos).

10.4 Acuerdos con otras organizaciones: los datos e información no pueden ser compartidos o entregados a Terceros (proveedores, instituciones, consultoras, investigadores, etc.) a no ser que se estén realizando acciones conjuntas, estudios o análisis, y exista un contrato, convenio o acuerdo de confidencialidad que asegure la reserva, protección de datos o secreto de la información compartida, resguardando reconocer la clasificación y las normas para su manipulación como también los mecanismos de traspaso seguro.

10.5 Registro de proveedores y terceros con acceso a Datos Se deberá registrar de manera oportuna en la sección de registros y declaraciones institucionales formulario “Proveedores o Terceros con acceso a Datos personales”, disponible en la intranet Institucional/Dirección de Gobierno de Datos y Análisis Institucional (link Declaraciones y Registros Institucionales (sharepoint.com), todo traspaso de datos a terceros identificando claramente el nombre de la persona o representante legal, RUN o RUT y objetivo del traspaso. Este traspaso siempre

debe estar amparado en un contrato, convenio o acuerdo de confidencialidad que explícitamente considere el tratamiento de este tipo de datos.

10.6 Copias de respaldo clasificadas: Si existieran, deben presentar un nivel de clasificación consistente con la información original.

10.7 Para copiar o imprimir un documento con información de carácter confidencial o reservado: Si no está dentro de sus funciones, se debe solicitar la autorización del dueño del documento.

10.8 En caso de tener dudas o consultas respecto al acceso o tratamiento de datos e información institucional, deben dirigir sus consultas a gobiernodedatos@duoc.cl

11. CONTROL Y SANCIONES AL INCUMPLIMIENTO

El incumplimiento de lo definido en esta política será considerado una falta grave, y podrá ser sancionado de acuerdo a la gravedad de ésta, previa evaluación de la intencionalidad, impacto y daño que cause a Duoc UC, según lo indicado en el Código de Ética y Conducta Duoc UC, Reglamento Interno de Higiene y Seguridad y las demás normativas institucionales.

12. DOCUMENTOS DE REFERENCIA

- Código de Ética y Conducta de la Fundación Instituto Profesional Duoc UC
- Reglamento Interno de Higiene y Seguridad y demás normativa institucional aplicable.
- Política de Gobierno de Datos
- Instructivo para aplicar Mecanismo Seguro de Traspaso de Datos

13. DIFUSIÓN Y COMUNICACIÓN DE LA POLÍTICA

La presente política debe ser debidamente comunicada a todos los colaboradores/as de Duoc UC.

Para estos efectos y para dar cumplimiento a lo anteriormente mencionado, se debe cumplir con un plan comunicacional y se debe disponer del presente instrumento para su debida difusión y divulgación interna.

La presente política quedará disponible para consultas en la plataforma documental de Gobierno de Datos (SharePoint).