

POLÍTICA DE GOBIERNO Y GESTIÓN DE DATOS INSTITUCIONALES

INSTITUTO PROFESIONAL SAN SEBASTIÁN (IPSS)

1. PROPÓSITO Y OBJETIVOS

La presente Política de Gobierno de Datos tiene como propósito establecer el marco normativo y estratégico que rige la captura, acceso, almacenamiento, procesamiento, uso y protección de los datos institucionales del Instituto Profesional San Sebastián (IPSS), así como los roles y responsabilidades asociados. El objetivo principal es asegurar que los datos sean tratados como un activo estratégico, garantizando su calidad, integridad, veracidad, seguridad y disponibilidad oportuna para facilitar la toma de decisiones basada en evidencia, la autorregulación, el aseguramiento de la calidad, la eficiencia en el control de gestión y el cumplimiento regulatorio.

2. NORMAS RELACIONADAS Y DEFINICIONES

La presente Política se enmarca en la normativa legal vigente que regula el uso y la protección de datos, así como en las políticas y normas institucionales que resulten aplicables. Especialmente conforman este marco legal y normativo:

- Constitución Política de la República, Artículo 19, N ° 4
- Ley N ° 21.719, de Protección de Datos Personales (vigente de forma progresiva desde su publicación).
- Ley N ° 19.628, Sobre Protección de la Vida Privada.
- Ley N ° 21.663, Ley Marco de Ciberseguridad
- Ley N ° 21.459, Ley de Delitos Informáticos
- Código del Trabajo, Artículo 154 bis
- Reglamento Interno de Orden, Higiene y Seguridad IPSS
- Código de Ética IPSS
- Reglamento Académico IPSS
- Política institucional de ciberseguridad de la información (por aprobar).
- Protocolo Interno de Gestión de Derechos de los Titulares de Datos Personales de IPSS (por aprobar).
- Normativa del Sistema Nacional de Aseguramiento de la Calidad de la Educación Superior (CNA, CNED, SIES), en tanto regulan los datos institucionales que deben ser reportados o acreditados.

Para efectos de esta Política, así como de las normas, reglamentos, instrucciones o procedimientos institucionales que de ella se deriven, se entenderá que los conceptos que se indican a continuación tendrán el significado que en cada caso se establece.

Definiciones clave

Datos: los datos son representaciones de hechos, expresados mediante textos, números, gráficos, imágenes, sonidos o videos, y pueden ser capturados y almacenados.

Dato institucional: todo dato generado, procesado, administrado o custodiado por el IPSS en el ejercicio de sus funciones académicas, administrativas, financieras o de gestión, con independencia de si está o no asociado a una persona natural.

Dato personal: cualquier información vinculada o referida a una persona natural identificada o inidentificable, conforme a la definición establecida por la Ley N° 21.719.

Dato personal sensible: dato personal que pertenece a categorías especialmente protegidas por ley, por tratar de la esfera más íntima de sus titulares —como datos de salud, origen étnico, orientación sexual, identidad de género o datos biométricos—, cuyo tratamiento por regla general está prohibido, salvo excepciones legales o autorización específica y explícita del titular, en condiciones reforzadas de protección.

Información: la información son datos en un contexto, de manera que esta contribuye al conocimiento, comprensión y conciencia de un determinado fenómeno.

Gobernanza de Datos: corresponde al conjunto de personas, procesos y tecnologías que permiten a la institución capturar, mantener, y gestionar los datos de su actividad de forma fiable y eficiente, para asegurar su veracidad, integridad, confidencialidad y disponibilidad, en orden a que estos contribuyan a la institución a tomar las decisiones oportunas en el momento adecuado.

Calidad de datos: hace referencia a un modelo que considera la precisión, integridad, vigencia y consistencia.

Accesibilidad: se refiere a que los usuarios autorizados puedan acceder de forma oportuna, segura y adecuada a los datos e información institucional necesarios para el cumplimiento de sus funciones, resguardando los permisos, la confidencialidad y la protección de datos sensibles.

Seguridad: permite garantizar la privacidad, confidencialidad y el acceso adecuado a los datos.

Dominio de datos: corresponde al conjunto de conceptos institucionales agrupados en torno a una misma materia, proceso, área o vista de gestión de la institución, permitiendo organizar y administrar de manera coherente los datos asociados a dicho ámbito.

Metadatos: los metadatos corresponden a datos que proporcionan información adicional sobre otros datos. Son descripciones que ayudan a entender, organizar y gestionar los datos de manera efectiva. Los metadatos brindan contexto sobre el contenido, la estructura, el significado y las relaciones de los datos.

Data Warehouse Institucional: base de datos centralizada y optimizada, diseñada para almacenar grandes volúmenes de información provenientes de variadas fuentes de datos, en un formato que sea fácil de consultar y analizar. Su objetivo es proporcionar un repositorio único y organizado donde los datos se almacenan de manera estructurada y se pueda acceder a ellos de manera eficiente para tomar decisiones informadas, así como la elaboración oportuna de reportes y análisis, entre otros.

Data Lake Institucional: es un repositorio centralizado y flexible, diseñado para almacenar grandes volúmenes de información provenientes de diversas fuentes de datos, en su formato original o con un bajo nivel de procesamiento previo. A diferencia de un Data Warehouse, que organiza los datos en estructuras definidas para su consulta y análisis, el Data Lake permite conservar datos estructurados, semiestructurados y no

estructurados¹, tales como bases transaccionales, archivos, registros, encuestas, documentos, textos, imágenes u otras fuentes institucionales.

Uso de datos: cualquier acción, consulta, explotación, análisis o aplicación de los datos.

Tratamiento de datos: cualquier operación, procedimiento técnico o conjunto de operaciones (automatizadas o no) que se realicen sobre datos personales.

Procesamiento de datos: conjunto de operaciones lógicas y automatizadas aplicadas a los datos, tales como la recolección, registro, organización, modificación, cruce o destrucción.

Propiedad del dato: derechos legales de autoría sobre los datos creados.

Arquitectura de datos: modelos, políticas y reglas que gobiernan cómo se estructuran los datos.

3. ALCANCE

Esta política es de cumplimiento obligatorio para todas las autoridades, directivos, docentes, estudiantes y colaboradores administrativos que interactúen, administren, procesen, traten, almacenen o usen, de cualquier forma, datos provenientes de los sistemas de información institucionales (como registro académico, entorno virtual de aprendizajes, sistemas financieros y plataformas de reportería, entre otros). También será de cumplimiento obligatorio para terceros que, con la debida autorización y dentro de la normativa legal e institucional vigente, tengan acceso a datos institucionales, para su uso o tratamiento. Los contratos o convenios con terceros proveedores de servicios que involucren acceso o tratamiento de datos institucionales deberán incorporar cláusulas de confidencialidad y las obligaciones que se deriven de la presente Política.

4. PRINCIPIOS RECTORES

- **Dato como Activo Institucional:** los datos críticos de la institución deberán ser gestionados como activos estratégicos, resguardando su consistencia, trazabilidad, calidad y uso adecuado en los distintos procesos académicos y administrativos. Para cada dominio de datos se deberá definir cuál es el dato oficial disponible para la gestión institucional, identificando su origen, responsable, reglas de validación, periodicidad de actualización y criterios de uso. Para ello deberá quedar documentado en un catálogo o glosario² institucional de datos, con el propósito de evitar duplicidades, interpretaciones divergentes y silos de información entre unidades, favoreciendo una toma de decisiones basada en información confiable, comparable y oportunamente disponible.
- **Calidad desde el Origen:** la exactitud, pertinencia y actualización de los datos se deben garantizar desde el momento de su captura en los sistemas transaccionales.

¹ Los datos pueden clasificarse en estructurados, cuando están organizados en tablas o campos definidos; semiestructurados, cuando poseen cierta organización mediante etiquetas, formularios o metadatos; y no estructurados, cuando no tienen una estructura predefinida, como textos abiertos, documentos, imágenes, audios o videos.

² Un glosario de datos estandariza la definición e interpretación de los conceptos institucionales, y el catálogo de datos documenta dónde está el dato, cómo se construye, quién es responsable, con qué periodicidad se actualiza y bajo qué reglas debe utilizarse.

- **Accesibilidad y Transparencia:** los datos deben estar disponibles de manera oportuna para los usuarios autorizados y los distintos perfiles de acceso definidos, estructurados en paneles e indicadores que faciliten la gestión.
- **Seguridad y Confidencialidad:** el tratamiento y uso de los datos debe cumplir con la normativa legal vigente sobre protección de datos personales y los estándares de ciberseguridad del IPSS. Asimismo, el almacenamiento debe efectuarse bajo condiciones óptimas de seguridad, garantizando la disponibilidad, integridad y confidencialidad de la información histórica y activa de la Institución.
- **Uso ético:** los datos deberán gestionarse de manera responsable, dando cumplimiento a la normativa legal vigente, marco regulatorio interno y a los principios rectores de esta política, para uso académico y de gestión institucional, garantizando siempre la privacidad, la equidad y el consentimiento de las personas. El uso debe estar estrictamente alineado con los permisos otorgados y las normativas de privacidad vigentes.

5. ROLES Y RESPONSABILIDADES

Para la correcta implementación de esta política, se define la siguiente estructura de roles y responsabilidades:

Responsables de Dominio de Datos: corresponde a administradores o usuarios funcionales cuyo conocimiento sobre un dominio específico les permite controlar los valores de datos referenciales y establecer reglas institucionales de calidad y uso. Se trata de un rol funcional interno, distinto del rol del responsable del tratamiento de dichos datos o de quién tiene el vínculo con el usuario o tercero y ha sido mandatado por el responsable del tratamiento.

Rol Estratégico del Gobierno de Datos: Corresponde a la Junta Directiva de la Institución, como instancia máxima de aprobación estratégica, que aprueba la política y sus modificaciones, supervisa los riesgos principales y recibe la rendición de cuentas.

Rol Ejecutivo del Gobierno de Datos (Nivel Patrocinador): instancia máxima de aprobación estratégica. Corresponde al Comité de Rectoría, que, liderado por el Rector, sanciona las políticas y evalúa el impacto del gobierno de datos cruzando con los objetivos del Plan de Desarrollo Estratégico.

Comité de Gobernanza de Datos (Nivel Táctico-operativo): equipo responsable de recoger, sancionar y resolver los requerimientos y necesidades sobre datos institucionales y sus respectivos indicadores, entregando lineamientos estratégicos en materias de riesgos, sistemas de información, normativa, aseguramiento de la calidad, entre otras. Está integrado por quienes ejerzan la titularidad de la Vicerrectoría de Asuntos Económicos, quién lo presidirá, la Secretaría General, la Dirección de Sistemas y Tecnologías, la Dirección de Análisis Institucional y Estudios, y la Dirección de Gestión y Presupuesto.

Además, el Comité de Gobernanza de Datos tendrá un rol de generación de cultura institucional en relación con la concientización de la comunidad educativa sobre el valor del dato y potenciales riesgos asociados.

Este Comité dictará su reglamento de funcionamiento y establecerá un plan de trabajo periódico, sobre el que reportará al Comité de Rectoría cuando le sea requerido y que incluirá acciones de formación y cultura institucional en materia de datos.

El Comité rendirá cuenta en forma periódica a la Junta Directiva sobre los avances y brechas del plan de trabajo, incluyendo eventuales incidentes relevantes y riesgos críticos asociados.

Equipo Técnico de Datos (Nivel operativo): equipo de desarrollo liderado por quien ejerza la Dirección de Análisis Institucional y Estudios, e integrado por representantes de las áreas de Sistemas y Tecnologías, y por otras personas convocadas ad hoc. Será responsable de la implementación y el despliegue del Gobierno de Datos.

6. CICLO DE VIDA Y ESTANDARIZACIÓN DEL DATO

6.1. Creación, captura y registro: los datos que alimentan los tableros e indicadores institucionales deberán originarse en procesos documentados, trazables y validados. Para los indicadores estratégicos o críticos, se deberá disponer de una Ficha Técnica del Indicador y de un Diccionario de Datos³ asociado, que permitan identificar su definición, fórmula de cálculo, variables utilizadas, fuente institucional validada, responsable, periodicidad de actualización, reglas de calidad, criterios de interpretación y acciones esperadas frente a desviaciones.

6.2. Almacenamiento y arquitectura de datos: los sistemas de almacenamiento y la arquitectura de datos del IPSS deberán ser seguros, escalables y adecuados al volumen, sensibilidad y uso de la información. Su definición deberá considerar disponibilidad, integridad, confidencialidad, respaldo, rendimiento, costo-eficiencia y alineación con los estándares tecnológicos institucionales.

6.3. Procesamiento y transformación: el procesamiento, integración, limpieza, estandarización, automatización o transformación de datos deberá realizarse para fines institucionales definidos, tales como mejorar la operación, asegurar la calidad de la información, cumplir obligaciones regulatorias, fortalecer la seguridad o apoyar la toma de decisiones. Todo tratamiento deberá efectuarse conforme a la legislación vigente, estándares éticos institucionales y principios de la presente Política.

6.4. Uso y análisis: el acceso, consumo y uso de información en tableros, reportes, soluciones de BI, modelos analíticos, modelos de IA o auditorías deberá realizarse por usuarios autorizados, para fines institucionales legítimos y definidos, asegurando trazabilidad, confidencialidad, pertinencia y cumplimiento normativo.

Los resultados de modelos analíticos o de inteligencia artificial deberán contar con supervisión humana por parte del responsable del dominio de datos, de forma previa a cualquier operación de tratamiento o aplicación práctica, de manera de garantizar la calidad de los datos, prevenir sesgos y evitar riesgos.

6.5. Conservación, retención y archivo: la conservación, retención y archivo de datos e información deberá considerar los plazos legales, regulatorios, contractuales,

³ La Ficha Técnica del Indicador explica el indicador y su forma de cálculo; el Diccionario de Datos describe las variables que lo componen; el Glosario de Datos estandariza el significado institucional de los conceptos; y el Catálogo de Datos documenta dónde está cada dato, quién lo gestiona, cómo se actualiza y bajo qué reglas se utiliza.

académicos, administrativos o institucionales que correspondan, así como su criticidad, sensibilidad, valor institucional y riesgos asociados a su mantención o eliminación.

6.6. Eliminación, destrucción y purga: corresponde al proceso mediante el cual la institución elimina de forma segura y controlada aquellos datos, archivos, copias o registros que ya cumplieron su finalidad y que no deben conservarse por razones legales, regulatorias, académicas, administrativas o institucionales. Por ejemplo, podrán eliminarse bases temporales de trabajo, archivos duplicados, respaldos operativos vencidos o copias con datos personales utilizadas en procesos ya cerrados, siempre que exista autorización, trazabilidad y resguardo de que no se afectará información oficial, histórica o probatoria de la institución. No se trata de “borrar datos institucionales importantes”, sino de gestionar responsablemente el cierre del ciclo de vida del dato.

7. INSTRUMENTOS COMPLEMENTARIOS

Para la implementación y verificación de la presente Política, el Comité de Gobernanza de Datos y el Equipo Técnico deberán elaborar y/o mantener actualizados los siguientes instrumentos complementarios, que formarán parte del gobierno de datos institucional:

- Catálogo institucional y glosario de datos.
- Diccionarios de datos y fichas técnicas de indicadores.
- Matriz de Propietarios Funcionales del Dato por dominio y sistema de información.
- Norma de clasificación de la información y gestión de accesos.
- Tabla institucional de retención, archivo y eliminación.
- Procedimientos de gestión de incidentes, solicitudes de titulares y tratamiento por terceros.
- Protocolo para analítica avanzada e inteligencia artificial.

La prioridad y plazos de elaboración de cada instrumento se establecerá en función de la etapa institucional de instalación del gobierno de datos y de las necesidades operativas del ciclo de implementación.

8. VIGENCIA Y ACTUALIZACIÓN DE LA POLÍTICA

La presente Política de Gobierno y Gestión de Datos Institucionales corresponde a una actualización efectuada a partir de un proceso de revisión y análisis respecto de los elementos que la conforman, permitiendo robustecer su despliegue de forma integral y alineada a los nuevos desafíos institucionales en la fase de consolidación del plan de desarrollo.

Como parte de los procesos de mejora continua, esta política es revisada en forma periódica o cuando existan cambios significativos en la estructura o sistemas del IPSS.

Esta política entrará en vigencia una vez aprobada por las instancias institucionales correspondientes e informada a la comunidad educativa. En caso de dudas sobre su interpretación, resolverá la Secretaría General, oyendo al Comité de Gobernanza de Datos.