

PROTECCIÓN DE DATOS PERSONALES EN LA UNIVERSIDAD DE VALPARAÍSO

INTRODUCCIÓN

En la Universidad de Valparaíso, resguardamos el derecho a la privacidad y el derecho fundamental a la protección de datos personales de todas las personas con las que nos relacionamos: estudiantes, académicos, funcionarios y colaboradores. El tratamiento de datos personales es una tarea cotidiana en nuestras unidades administrativas y académicas; por ello, todos tenemos el deber de conocer y aplicar las normas vigentes, especialmente la Ley N.º 19.628 sobre Protección de la Vida Privada, que regula el tratamiento de estos datos por organismos públicos y privados

Cada vez que elaboramos un documento, planilla o publicación que contiene información personal, nos convertimos en guardianes de los datos personales de nuestra comunidad.

1. DEFINICIONES BÁSICAS

Dato personal: Toda información relacionada con una persona natural identificada o identificable, como RUT, correo electrónico institucional o domicilio.

Dato sensible: Información que se refiere a aspectos privados o íntimos, como salud física o psíquica, ideología, religión, origen racial o vida sexual. Su tratamiento está generalmente prohibido, salvo excepciones legales.

Ejemplos:

- ✓ Publicar nombre, cargo y remuneración de funcionarios en Transparencia Activa (obligación legal).
- ✗ Publicar su AFP, sistema de salud o cuenta bancaria (dato sensible o innecesario).

2. TRATAMIENTO DE DATOS

Por regla general, el tratamiento de datos personales requiere consentimiento del titular. Sin embargo, los organismos públicos pueden tratar datos personales sin ese consentimiento cuando actúan dentro de sus competencias legales (por ejemplo, al cumplir la Ley de Transparencia)

Todo tratamiento debe cumplir los principios de finalidad (uso solo para fines autorizados), proporcionalidad (publicar solo lo estrictamente necesario, adecuado y relevante para dichos fines) y seguridad.

3. OBLIGACIONES PRINCIPALES DE QUIENES TRATAN DATOS

Recolección legítima: Solo obtener datos necesarios para fines legales o institucionales.

Exactitud y actualización: Verificar que la información sea correcta y esté al día; corregir errores oportunamente.

Minimización: Recopilar, utilizar y conservar solo los datos personales que sean estrictamente necesarios y adecuados para un fin específico y legítimo.

Reserva y secreto: Mantener confidencialidad respecto de datos no públicos, incluso después de dejar el cargo.

Limitación de acceso: Compartir datos personales únicamente con quienes estén autorizados o tengan competencia legal.

Eliminación o bloqueo: Cuando los datos sean erróneos, caducos o se usen indebidamente, deben eliminarse o bloquearse.

4. EJERCICIO DE DERECHOS

Los titulares de los datos podrán ejercer sus derechos de acceso, actualización, rectificación y oposición al tratamiento de datos.

CONCLUSIÓN

La protección de datos personales es una responsabilidad compartida que garantiza el respeto este derecho fundamental y fortalece la confianza en nuestra institución. Cumplir estas normas no es solo una exigencia legal, sino también una práctica ética fundamental para toda comunidad universitaria.

Para consultas o asesoría específica, puedes contactar a la Unidad de Transparencia y Gestión Documental.