

# Protección de datos personales en edificios: ¿qué deben saber las juntas de propietarios?

La protección de datos personales no es un tema nuevo en el Perú. Desde la promulgación de la Ley N.º 29733, de Protección de Datos Personales, el 3 de julio del 2011, su aplicación se ha extendido más allá del ámbito empresarial, abarcando también entornos cotidianos como edificios residenciales y condominios.

En marzo de este año, la Autoridad Nacional de Protección de Datos Personales –órgano adscrito al Ministerio de Justicia y Derechos Humanos (Minjusdh)– publicó la «**Guía práctica para el tratamiento de datos personales por juntas de propietarios y administradores de edificios**». Este documento orienta a los responsables de la gestión de inmuebles residenciales sobre el adecuado manejo de los datos personales, conforme a la legislación vigente.

## Escenarios cotidianos con implicancia legal

Muchas prácticas habituales en edificios pueden vulnerar la privacidad de las personas sin que sus responsables lo adviertan:

- Solicitar el DNI a visitantes o retenerlo a cambio de un fotocheck.

- Publicar listas de vecinos morosos en áreas comunes.
- No actualizar canales de comunicación pese a solicitudes expresas.
- Filtrar datos en grupos de WhatsApp, provocando la recepción de mensajes no deseados.

Estas situaciones, aparentemente inofensivas, pueden constituir infracciones a la normativa de protección de datos personales, cuya aplicación también rige para las relaciones vecinales y administrativas.

## **Aspectos claves de la guía para juntas de propietarios**

La guía ofrece una serie de lineamientos para asegurar el cumplimiento normativo y evitar vulneraciones en el tratamiento de datos.

### **1. Responsabilidad del tratamiento**

La Junta de Propietarios, siempre que esté inscrita en Registros Públicos, asume el rol de responsable del tratamiento de los datos personales recolectados. Sus miembros deben cumplir con los deberes establecidos por ley, al igual que cualquier organización o empresa.

### **2. ¿Qué es un dato personal?**

Se considera dato personal cualquier información que permita identificar a una persona a través de medios razonablemente utilizables. Algunos ejemplos en el ámbito residencial son:

- Nombres de propietarios, residentes o visitantes.
- Correos electrónicos y números telefónicos.
- Documentos de identidad.
- Números de departamentos.
- Cuentas bancarias empleadas para pagos.
- Registros de visitas o grabaciones de videovigilancia.

### **3. Consentimiento informado**

Toda recolección de datos debe estar sustentada en el consentimiento informado del titular. Para ello, se recomienda el uso de cartillas informativas que especifiquen claramente las finalidades, como:

- Control de accesos.
- Administración y cobro de cuotas de mantenimiento.
- Envío de alertas de seguridad.
- Comunicaciones internas.
- Cumplimiento de obligaciones contractuales

### **4. Derechos ARCO**

Las juntas deben habilitar mecanismos accesibles que permitan a los titulares ejercer los derechos ARCO: Acceso, Rectificación, Cancelación y Oposición al tratamiento de sus datos. Estos procedimientos deben comunicarse a todos los residentes.

### **5. Medidas de seguridad**

Es imprescindible aplicar medidas de seguridad técnicas y organizativas, tales como:

- Actualización periódica de contraseñas.

- Uso de cerraduras físicas para archivos.
- Protección de dispositivos electrónicos que almacenen datos sensibles.

## **6. Prácticas prohibidas**

La guía prohíbe expresamente la retención o fotocopiado del DNI como condición de ingreso. Este documento contiene información sensible que puede ser utilizada de forma indebida, especialmente en entornos digitales.

El uso de datos biométricos solo se justifica en casos específicos y con consentimiento explícito. Sin embargo, su aplicación en visitas ocasionales está descartada.

## **7. Rol del administrador**

El administrador del edificio actúa como encargado del tratamiento de datos, siempre bajo las instrucciones de la Junta de Propietarios, quien conserva la responsabilidad legal principal.

## **8. Registro de bancos de datos**

Toda junta debe registrar ante el Minjusdh los bancos de datos personales que gestione. Este registro no implica entregar la base de datos, sino completar un formulario que detalle la naturaleza de la información contenida, como:

- Datos de propietarios, inquilinos y proveedores.
- Registros de visitas o de incidencias.
- Información obtenida mediante videovigilancia.

## **9. Uso de cámaras de seguridad**

En el caso de videovigilancia, se exige la colocación de avisos visibles que informen sobre:

- La existencia del sistema.
- Finalidad de las grabaciones.
- La identidad del responsable del tratamiento.

Estos carteles deben ubicarse en zonas estratégicas, de fácil visualización para residentes y visitantes.