

Checklist de seguridad de la información

Revisión rápida de las medidas que protegen los datos de residentes, familias y trabajadores, en papel y en formato digital.

Normativa de referencia: Ley 21.719 (Ley 19.628 modificada); Ley 20.584; Decreto 41 de 2012 del Ministerio de Salud, artículo 9; Decreto 20 de 2021 del Ministerio de Salud, artículos 29 letra e) y 30. Documento referencial: válidalo antes de usarlo.

Cómo usar este checklist

La Ley 21.719 entra en vigencia el 1 de diciembre de 2026 y exige, entre otras cosas, aplicar medidas de seguridad adecuadas al riesgo, que pueden incluir revisar su eficacia en forma regular. Ante un incidente, la residencia debe poder demostrar las medidas que aplicó. Este checklist te ayuda a revisar las más importantes para una residencia; no reemplaza la asesoría legal.

Marca **Sí** o **No** en cada medida. Por cada «No», anota quién se hace cargo y en qué plazo. Repite la revisión cada _____ meses (recomendamos dos veces al año) y guarda cada versión completada: es tu evidencia.

ESTABLECIMIENTO

FECHA

COMPLETADO POR (NOMBRE Y CARGO)

PRÓXIMA REVISIÓN

1. Organización

Medida	Sí	No	Responsable y plazo
Hay un(a) coordinador(a) de protección de datos, designado(a) por escrito: _____.			
La residencia tiene una política de protección de datos (MACA-DAT-01) aprobada y conocida por el equipo.			
La política está a disposición del público, con fecha y versión, en el sitio web de la residencia o en otro medio equivalente.			
Existe un registro de actividades de tratamiento (MACA-DAT-07), revisado en los últimos 12 meses.			
Se revisó con el asesor si corresponde una evaluación de impacto en protección de datos (por ejemplo, por tratar datos de salud sin consentimiento).			
Todo el equipo recibió capacitación en protección de datos este año, con registro firmado.			
Todo el personal, incluidos reemplazos, practicantes y voluntarios, firmó el compromiso de confidencialidad (MACA-DAT-04).			

2. Documentos en papel

Medida	Sí	No	Responsable y plazo
Las carpetas personales se guardan bajo llave, y la llave la tienen solo personas autorizadas.			
Escritorio limpio: al terminar el turno no quedan carpetas, recetas ni listados a la vista.			
Las pizarras y diarios murales de pasillos y espacios comunes no muestran diagnósticos, medicamentos ni otros datos de salud.			
El préstamo y la salida de carpetas quedan anotados en el registro de acceso (MACA-DAT-09).			
Los papeles con datos personales se eliminan con trituradora o empresa certificada, nunca en la basura común.			

3. Equipos y cuentas

Medida	Sí	No	Responsable y plazo
Cada persona tiene su propia clave en computadores y sistemas. Nadie comparte claves ni las deja anotadas a la vista.			
Los computadores se bloquean solos tras _____ minutos sin uso, y el equipo los bloquea al alejarse.			
Todos los equipos tienen antivirus activo y actualizaciones automáticas.			
El correo y los sistemas con datos de residentes usan verificación en dos pasos.			
Hay respaldo periódico de la información, y se probó recuperarlo en los últimos _____ meses.			
El wifi de visitas está separado de la red que usan los equipos de la residencia.			
Cuando un trabajador deja la residencia, se le quitan sus claves y accesos el mismo día.			

4. Celulares y mensajería

Medida	Sí	No	Responsable y plazo
El personal no guarda fotos de residentes en sus celulares personales.			
Los grupos de WhatsApp del equipo y con familias no se usan para datos clínicos ni diagnósticos.			
El celular institucional tiene bloqueo con clave o huella y se puede localizar o borrar a distancia.			
La información de salud se envía a la familia solo por el canal acordado y a la persona autorizada.			

5. Proveedores

Medida	Sí	No	Responsable y plazo
Los proveedores que tratan datos por encargo (software, contabilidad, informática, nube, cámaras) firmaron un contrato o anexo de encargo (MACA-DAT-06).			
Se sabe en qué país guarda los datos cada proveedor y, si es fuera de Chile, hay garantías adecuadas para esa transferencia.			
El software de la residencia tiene perfiles por rol: cada persona ve solo lo que necesita para su trabajo.			
El software guarda un registro de accesos: quién entró, cuándo y qué revisó (Decreto 41 de 2012, art. 9).			

6. Derechos y brechas

Medida	Sí	No	Responsable y plazo
Hay un procedimiento para responder solicitudes de acceso, rectificación, supresión, oposición, portabilidad y bloqueo en 30 días corridos (bloqueo: 2 días hábiles), con un responsable y un formulario (MACA-DAT-05).			
Existe un protocolo ante brechas de seguridad (MACA-DAT-08): el equipo sabe a quién avisar y la dirección sabe cuándo reportar a la Agencia y avisar a cada persona afectada.			
Se lleva un registro de incidentes, que incluye las brechas que no se comunicaron a la Agencia.			

7. Residentes y familias

Medida	Sí	No	Responsable y plazo
Cada residente o su representante recibió información sobre qué datos se usan y para qué, y firmó las autorizaciones que correspondan (MACA-DAT-02).			
Hay una autorización de uso de imagen firmada antes de publicar fotos (MACA-DAT-03), y se respeta a quien no autoriza.			
La información de salud se entrega solo al residente, a su representante o a las personas que él autorizó.			

Resultado

Cuenta las medidas marcadas con «Sí» y elige las tres que vas a resolver primero.

MEDIDAS CUMPLIDAS (DE 33)

TRES PRIORIDADES PARA LOS PRÓXIMOS TRES MESES

Coordinador(a) de protección de datos

Director(a) técnico(a)

Fecha

Haz también el **test de protección de datos de MACA** en macainn.cl/recursos: es gratis, no pide registro y te entrega un informe en PDF con lo que le falta a tu residencia.