

Accesos por función

Adecuación Ley 21.719

Cambio organizacional

Desarrollo organizacional

GUÍA NOVALIS · SERIE ADECUACIÓN · LEY 21.719

El acceso sigue a la función

Quién puede ver qué información no se define por confianza ni por antigüedad: se deriva de la función de cada cargo.

La pregunta

En la mayoría de las organizaciones, el acceso a la información se distribuyó por historia: quién llegó primero, quién es de confianza, quién lo pidió alguna vez. Nadie lo diseñó. La pregunta que casi nadie se hace: **¿cuántos de los accesos vigentes resistirían la pregunta “¿para qué lo necesita su función?”**

Lo que dice la ley

El principio de proporcionalidad (art. 3 letra c) establece que solo deben tratarse los datos necesarios para la finalidad declarada, y el de seguridad (art. 3 letra f) exige resguardos proporcionales al riesgo. Aplicados al interior de la organización, ambos dicen lo mismo: **cada función accede a la información que su propósito requiere** — ni más, ni por costumbre.

Art. 3 c Proporcionalidad: solo los datos necesarios para el fin declarado. “Por si acaso” no es una finalidad.	16 campos El Registro de Actividades de Tratamiento documenta, entre otros, quién accede a cada dato y por qué.	20.000 UTM o el 4% de los ingresos: multa máxima cuando el mal manejo alcanza datos sensibles.	1 dic 2026 Vigencia plena de la ley. Los accesos heredados pasan a ser un riesgo documentable.
---	---	--	--

La escena

El acceso heredado

La clave que se comparte desde hace años. La carpeta que quedó abierta “por mientras”. El acceso que se dio para una tarea puntual y nadie retiró. Ninguno fue una decisión: se fueron acumulando, y lo acumulado se volvió invisible porque funcionaba. Hasta que alguien pregunta quién puede ver las remuneraciones, y la respuesta honesta es: **no lo sabemos con certeza.**

Qué hacer

- **Derivar los accesos desde las descripciones de cargo.** Qué información necesita cada función para cumplir su propósito — esa es la que debe tener.
- **Inventariar los accesos vigentes y compararlos con los necesarios.** La distancia entre ambos es el trabajo pendiente, y suele ser reveladora.
- **Cerrar por función, no por persona.** Retirar un acceso no es desconfiar de alguien: es ordenar el diseño.
- **Revisar cada vez que un cargo cambia.** Los accesos siguen a la función; cuando la función cambia, los accesos también.

Señales de alerta

Tu organización distribuye el acceso por historia, no por diseño, si:

- Existe al menos una clave compartida que “todos conocen”.
- Hay ex trabajadores cuyos accesos siguen vigentes.
- Nadie puede listar quién accede hoy a remuneraciones o datos de salud.
- Retirar un acceso se percibe como una ofensa personal.

El fondo

Definir los accesos por función obliga a precisar, muchas veces por primera vez en años, qué hace realmente cada función. Por eso este ejercicio ordena bastante más que los datos: deja a la vista el diseño real de la organización, con sus duplicidades y sus vacíos. La ley pide lo primero; el valor está en lo segundo.

Autoevaluación

Marca **Sí** en cada afirmación que tu organización ya tiene resuelta. Luego cuenta cuántas marcaste y lee el resultado.

¿Lo tienen resuelto?	Sí	No
1. Los accesos a información derivan de las descripciones de cargo, no de la historia.	☐	☐
2. Sabemos con exactitud quién puede ver remuneraciones, licencias y datos de clientes o socios.	☐	☐
3. No existen claves compartidas de uso colectivo.	☐	☐
4. Cuando alguien deja la organización, sus accesos se cierran el mismo día.	☐	☐
5. Cuando alguien cambia de función, sus accesos se revisan.	☐	☐
6. Las carpetas con datos personales tienen acceso restringido por función.	☐	☐
7. Los datos sensibles (salud, situación socioeconómica) tienen resguardo reforzado.	☐	☐
8. Proveedores y externos tienen accesos delimitados y con plazo.	☐	☐

9. Los sistemas permiten saber quién consultó qué información.

☐
☐

10. Podríamos justificar ante un tercero cada acceso vigente.

☐
☐

Lee tu resultado

- **8-10 marcadas** **Base sólida.** Los accesos tienen diseño. Revisa los puntos abiertos: suelen ser los primeros que una fiscalización encuentra.
- **5-7 marcadas** **Brechas relevantes.** El acceso heredado ya es un riesgo documentable. El tiempo alcanza si se parte ahora, con método.
- **0-4 marcadas** **Riesgo alto.** Hoy nadie podría explicar quién ve qué ni por qué. Es el momento de diseñar, no de seguir heredando.

¿Tus accesos resistirían la pregunta “¿para qué lo necesita su función?” Conversemos.

Si prefieres partir por tu cuenta: el **autodiagnóstico de 90 segundos** está en **novalis-21719.pplx.app** — una primera lectura de tu situación, sin registro.

Escríbeme a daniel@novalis.cl · Visita novalis.cl



Daniel Reffer Carrasco

Psicólogo Organizacional · Mg. Gestión de Personas
Consultor Organizacional · Docente Universitario

Guía · Serie Adecuación

Folio NOV-GU-002 · v1
Julio 2026

Próxima guía de la Serie Adecuación — **NOV-GU-003 · El correo era la base de datos**

Esta guía tiene fines informativos y no constituye asesoría jurídica. Se basa en la Ley 21.719 (vigencia plena: 1 de diciembre de 2026); conviene verificar siempre contra el texto oficial de la ley y sus reglamentos.