Políticas RLS

Conceptos Clave en las Políticas

auth.uid()

¿Qué es? Es tu número de identificación único cuando estás conectado.

Analogía: Es como tu número de estudiante en la escuela. Cada vez que entras, el sistema sabe quién eres.

USING

¿Qué hace? Define QUIÉN puede hacer algo.

Analogía: Es como la pregunta "¿Quién puede entrar?" en la puerta de un club.

WITH CHECK

¿Qué hace? Verifica que los datos nuevos cumplan las reglas.

Analogía: Es como un inspector que revisa que todo esté correcto antes de guardar.

EXISTS

¿Qué hace? Pregunta "¿Existe algo que cumpla esta condición?"

Analogía: Es como preguntar "¿Hay algún caramelo rojo en esta bolsa?"

rol = 'admin'

¿Qué es? Un rol especial que tiene permisos para hacer casi todo.

Analogía: Es como ser el maestro de la clase en lugar de un estudiante.

1. PERFILES (Tu Tarjeta de Identidad)

¿Qué son? Son como las tarjetas de identidad de cada usuario en la aplicación.

Políticas:

"Usuarios ven su perfil"

sql

```
USING (auth.uid() = id)
```

Explicación: Solo puedes ver TU propia tarjeta de identidad, no la de los demás.

Ejemplo: Si tu ID es "123", solo puedes ver el perfil "123", no el "456" ni el "789".

"Usuarios actualizan su perfil"

sql

```
USING (auth.uid() = id)
WITH CHECK (auth.uid() = id)
```

Explicación: Solo puedes cambiar la información de TU propia tarjeta.

Ejemplo: Puedes cambiar tu nombre, pero no puedes cambiar el nombre de otra persona.

"Admin acceso total a perfiles"

sql

```
USING (
  EXISTS (
    SELECT 1 FROM public.perfiles
    WHERE id = auth.uid() AND rol = 'admin'
  )
)
```

Explicación: Si eres el director de la escuela (admin), puedes ver y modificar TODAS las tarjetas de identidad.

2. CATEGORÍAS (Las tiquetas de los Productos)

¿Qué son? Son como las secciones de una tienda: "Juguetes", "Ropa", "Comida".

Políticas:

"Público ve categorías activas"

sql

```
USING (esta_activa = TRUE)
```

Explicación: Todos pueden ver las secciones de la tienda que están abiertas, pero no las que están cerradas o en construcción.

Ejemplo: Puedes ver "Deportivas" y "Trabajo", pero no "Categoría Experimental" porque aún no está activa.

"Admins gestionan categorías"

sql

```
USING (
  EXISTS (
    SELECT 1 FROM public.perfiles
    WHERE id = auth.uid() AND rol = 'admin'
  )
)
```

Explicación: Solo el dueño de la tienda (admin) puede crear nuevas secciones, cerrarlas o cambiarles el nombre.

3. PRODUCTOS (Las Motocicletas)

¿Qué son? Son los artículos que se venden en la tienda.

Políticas:

"Público ve productos activos"

sql

```
USING (
  esta_activo = TRUE
  OR
  EXISTS (
    SELECT 1 FROM public.perfiles
    WHERE id = auth.uid() AND rol = 'admin'
  )
)
```

Explicación:

- Los clientes normales solo ven las motos que están a la venta
- El dueño de la tienda puede ver TODAS las motos, incluso las que están guardadas en el almacén

Ejemplo: Tú ves "Yamaha R6" porque está activa, pero no ves "Moto en mantenimiento". El admin sí ve ambas.

"Admins gestionan productos"

Explicación: Solo el dueño puede agregar nuevas motos, cambiar precios o quitar motos del catálogo.

4. CARRITOS (Tu Carrito de Compras)

¿Qué es? Es como tu carrito del supermercado.

Políticas:

"Usuario gestiona su carrito"

sql

```
USING (auth.uid() = usuario_id)
WITH CHECK (auth.uid() = usuario_id)
```

Explicación: Solo TÚ puedes ver y modificar TU carrito. No puedes meter cosas en el carrito de otra persona ni ver qué está comprando.

Ejemplo: Si tu ID es "Juan", solo puedes ver el carrito de "Juan", no el de "María".

5. ITEMS DEL CARRITO (Los Productos en tu Carrito)

Políticas:

"Usuario gestiona sus items del carrito"

sql

```
USING (
  EXISTS (
    SELECT 1 FROM public.carritos c
    WHERE c.usuario_id = auth.uid() AND c.usuario_id = carrito_id
  )
)
```

Explicación: Solo puedes agregar, quitar o ver los productos que están en TU carrito.

Ejemplo: Pusiste 2 "Yamaha R6" en tu carrito. Solo tú puedes ver eso, cambiar la cantidad o quitarlas.

6. DIRECCIONES DE ENVÍO (Dónde Vives)

Políticas:

"Usuario gestiona sus direcciones"

sql

```
USING (auth.uid() = usuario_id)
WITH CHECK (auth.uid() = usuario_id)
```

Explicación: Solo TÚ puedes ver y cambiar tus direcciones de entrega. Nadie más puede ver dónde vives.

Ejemplo: Guardas tu dirección "Calle Falsa 123". Solo tú puedes verla y editarla.

7. PAGOS (Tus Pagos y Tarjetas)

Políticas:

"Usuarios ven sus pagos"

sql

```
USING (auth.uid() = usuario_id)
```

Explicación: Solo puedes ver TUS recibos de pago, no los de otras personas.

"Usuarios crean pagos"

sql

```
WITH CHECK (auth.uid() = usuario_id)
```

Explicación: Solo puedes crear pagos a TU nombre.

"Admins actualizan pagos"

Explicación: Solo el dueño de la tienda puede marcar un pago como "completado" o "reembolsado".

8. PEDIDOS (Tus Órdenes de Compra)

Políticas:

"Usuarios ven sus pedidos"

sql

```
USING (auth.uid() = usuario_id)
```

Explicación: Solo puedes ver TUS órdenes de compra, no las de otros clientes.

Ejemplo: Ves que compraste una "Honda CBR650R" el 15 de marzo, pero no ves lo que compró tu vecino.

"Usuarios crean pedidos"

sql

```
WITH CHECK (auth.uid() = usuario_id)
```

Explicación: Solo puedes crear pedidos a TU nombre.

"Admins ven todos los pedidos"

Explicación: El dueño de la tienda puede ver TODOS los pedidos de TODOS los clientes para poder procesarlos.

"Admins actualizan pedidos"

Explicación: Solo el dueño puede cambiar el estado de un pedido (de "pendiente" a "enviado" o "entregado").

9. ITEMS DEL PEDIDO (Los Productos que Compraste)

Políticas:

"Usuarios ven items de sus pedidos"

sql

```
USING (
  EXISTS (
    SELECT 1 FROM public.pedidos
    WHERE id = items_pedido.pedido_id AND usuario_id = auth.uid()
  )
)
```

Explicación: Solo puedes ver los detalles de los productos que TÚ compraste.

Ejemplo: Ves que tu pedido incluye "1 KTM Duke 390 a $130,000", pero no ves los productos del pedido de otra persona.