# Seguridad básica: ¿en qué consiste?

Implementa la seguridad de tu API Rest con Spring Boot

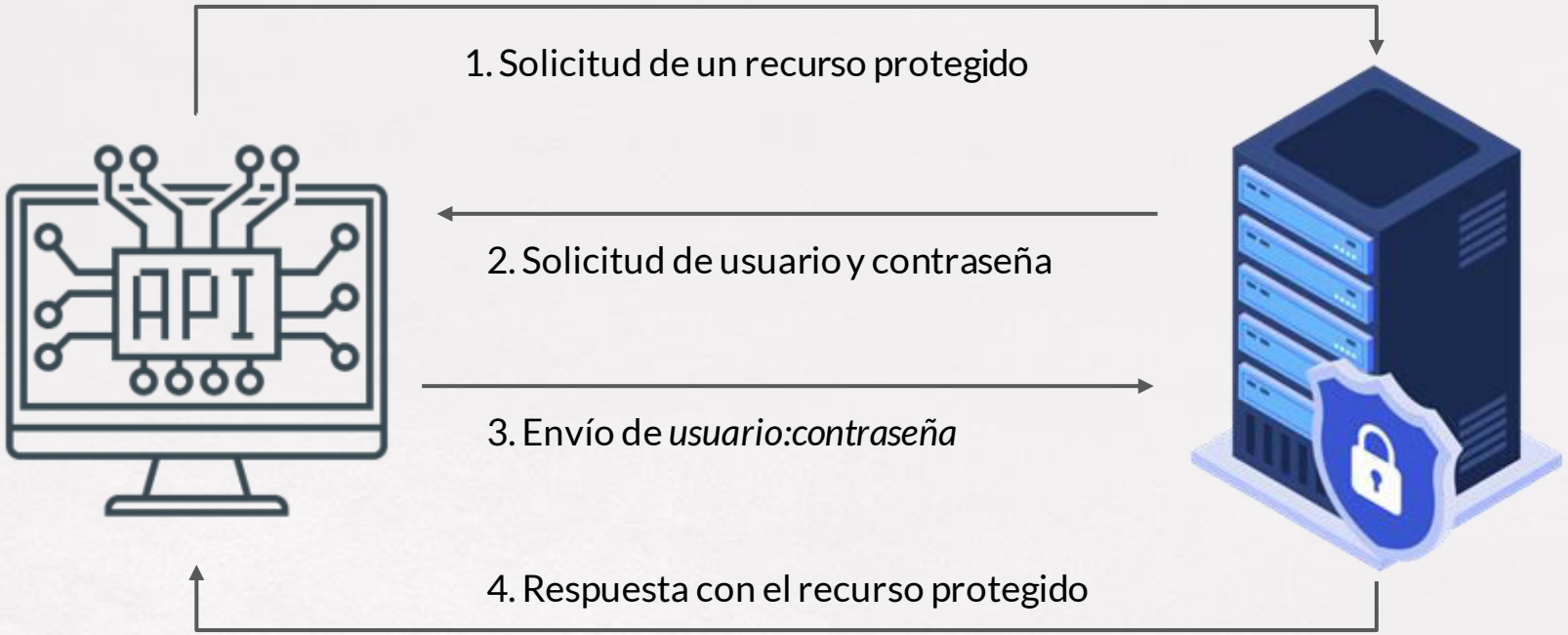
# Autenticación básica

- Método para que un cliente (o navegador web) pueda enviar las credenciales de un usuario (usuario y contraseña) al servidor.
- Definida en la especificación de HTTP (RFC 1945, RFC 2617)
- Simple de implementar, pero puede ser no adecuada en muchas situaciones.

# Autenticación básica

- No está pensado para canales públicos
- Las credenciales se envían en Base64 (no es un cifrado, solo una codificación).
- Si trabajamos con HTTP, “cualquiera” las podría descifrar.
- No obliga al uso de cookies ni de formularios de acceso.

# Autenticación básica



# Autenticación: lado cliente

- Se utiliza el encabezado *Authorization*
- La cabecera se construye siguiendo estos pasos
  - Se concatenan nombredeusuario, :, y constraseña
  - La cadena se codifica en Base64
  - el método de autorización es Basic, seguido de un espacio.
- Un ejemplo sería `Authorization: Basic dXNlcjoxMjM0` siendo las credenciales *user* y *1234*.

# Autenticación: respuesta del servidor

- Si la autenticación tiene éxito, se devuelve el recurso solicitado
- Si no, se debe devolver un código 401 No autorizado
- La respuesta incluirá además
  - Una cabecera WWW-Authenticate

```
WWW-Authenticate: Basic realm="TheRealm"
```

# *AuthenticationEntryPoint*

- Se invoca cuando la autenticación falla
- Implementación por defecto: *BasicAuthenticationEntryPoint*
- Podemos (y lo haremos) proporcionar nuestra propia implementación.
- Además del código de respuesta (401) y la cabecera indicada por el RFC correspondiente, enviaremos un mensaje de error JSON.