



Servidor MCP remoto que permite a Claude consultar y operar las instancias de ServiceNow que el cliente registra y controla. Esta ficha resume los controles de seguridad y el tratamiento de datos para las áreas de compras y de TI.

## Controles

### Credenciales cifradas

Las credenciales de cada instancia se cifran en reposo con Fernet (AES-128-CBC con HMAC), con una clave maestra que no vive en la base de datos. Nunca se muestran en el panel ni en las respuestas.

### Auditoría exportable

Cada ejecución queda registrada: herramienta, instancia, usuario, fecha, resultado y un resumen del payload sin credenciales. Se exporta a CSV.

### Confirmación en producción

Las instancias marcadas como producción piden confirmación explícita antes de cualquier escritura.

### OAuth 2.1 con PKCE

Claude se conecta con un flujo OAuth estándar con PKCE y registro dinámico de clientes. Los tokens caducan y se pueden revocar en cualquier momento.

### Lista de IPs

El endpoint MCP puede restringirse a direcciones o rangos autorizados, con fecha de caducidad.

### Roles mínimos

El usuario técnico solo tiene los roles que tú le asignes en ServiceNow. Recomendamos empezar en desarrollo o PDI.

## Datos que se almacenan

|                           |                                                                                           |
|---------------------------|-------------------------------------------------------------------------------------------|
| <b>Cuenta del panel</b>   | Correo, hash de contraseña (bcrypt), rol, fecha de creación y último acceso.              |
| <b>Instancias</b>         | Alias, URL, usuario técnico y credencial cifrada.                                         |
| <b>Autorización OAuth</b> | Clientes registrados, tokens de acceso y refresco, alcances e IP de origen.               |
| <b>Auditoría</b>          | Herramienta, instancia, usuario, fecha, resultado y resumen del payload sin credenciales. |
| <b>Memoria de trabajo</b> | Solo las observaciones que el usuario o el asistente guardan de forma explícita.          |
| <b>Caché</b>              | Metadatos de tablas y documentación pública de ServiceNow, con caducidad.                 |

## Lo que no se almacena

- El contenido de las conversaciones con el asistente.
- Los registros de ServiceNow que devuelve una consulta, salvo que el usuario los guarde como observación.
- Ningún dato se usa para publicidad, perfilado ni entrenamiento de modelos.

## Permisos en ServiceNow

El usuario técnico necesita el rol admin o, como mínimo, rest\_api\_explorer más los roles x\_mcp\_bridge.executor y x\_mcp\_bridge.script\_runner una vez instalado el bridge.

Marco legal: Ley 1581 de 2012 (Colombia). Licencia comercial de OPTIMO TECH S.A.S. Acuerdo de confidencialidad y DPA disponibles para empresas.

## Infraestructura y operación

- Tráfico solo por HTTPS.
- Panel con CSP, HSTS, X-Frame-Options y protección CSRF.
- Base de datos PostgreSQL bajo control de OPTIMO TECH S.A.S.
- Instancias sin uso por 30 días quedan invalidadas y exigen revalidación.
- Solicitudes de acceso, corrección o eliminación atendidas en máximo 30 días.