

API Gateway en adelante el PROVEEDOR declara el siguiente acuerdo de confidencialidad a favor del interesado, en adelante el CLIENTE.

Definiciones

1. **Firma electrónica:** archivo digital con datos de clave pública y privada de la firma electrónica de una persona natural en Chile. Lo llamado comúnmente “firma electrónica simple” que permite el acceso al SII. Junto a esta firma se encontrará la contraseña del archivo que permite abrir la firma.
2. **Credenciales SII:** RUT y contraseña del sitio del SII de la empresa y/o usuario que esté autorizando el ingreso con sus datos a su cuenta.
3. **Servicios de API Gateway:** cualquier servicio de API Gateway u otro asociado que el cliente esté usando donde se requiera usar la firma electrónica o credenciales del SII para realizar consultas al sitio web del SII y extraer datos o realizar acciones en este.

Cláusula Primera: el CLIENTE bajo su absoluta voluntad realiza el envío de uno o más documentos privados, credenciales, o archivos digitales (incluyendo la firma electrónica), para que el PROVEEDOR realice cierta labor en su nombre que involucra estos datos.

Cláusula Segunda: debido a la naturaleza del trabajo que se llevará a cabo, el PROVEEDOR tendrá acceso a información confidencial del cliente durante la ejecución de la actividad (desde que se entrega la firma o credenciales).

Cláusula Tercera: Datos que serán conocidos por el PROVEEDOR.

Los datos que el CLIENTE podría entregar al PROVEEDOR y que este contrato cubre son:

- Firma electrónica.
- Credenciales del SII.

Adicionalmente, el PROVEEDOR podrá conocer cualquier dato, al que se tenga acceso en el SII a través de la firma o credenciales del SII, que sea considerado necesario para la prestación del servicio solicitado.

Cláusula Cuarta: Propósito.

El PROVEEDOR usará los datos proporcionados por el CLIENTE para realizar alguna labor en su nombre. Por ejemplo, y sin ser un listado taxativo:

- Probar casos de uso de consultas que hoy no existan o que requieran una modificación solicitada por el CLIENTE para mejorar, corregir o crear una nueva funcionalidad en API Gateway.
- Generar documentos o ingresar datos en el SII que se hayan acordado previamente para la prestación del servicio y poder atender al CLIENTE.
- Reproducir casos de uso de servicios web de API Gateway para revisar comportamientos o errores informados por el CLIENTE.

La definición exacta del propósito de uso de los datos estará declarada en la solicitud de servicio que el CLIENTE haya solicitado al PROVEEDOR.

Cláusula Quinta: Duración de la autorización para uso de firma o credenciales SII.

El uso de la firma electrónica o credenciales SII será exclusivamente por el tiempo requerido para el servicio solicitado al PROVEEDOR. No pudiendo ser utilizados estos datos para otros fines que no sean los exclusivamente otorgados por el CLIENTE.

Para servicios de respaldos y obtención de datos desde el SII, se podrá utilizar la firma electrónica o credenciales para obtener cualquier dato que el CLIENTE haya solicitado u otros que el PROVEEDOR considere relevantes entregar al CLIENTE para prestar el servicio.

En ningún caso se hará uso de la firma o credenciales SII para emitir documentos con efecto real tributario, como por ejemplo: facturas o boletas de honorarios, en nombre del cliente y sin su expresa autorización. También se descarta cualquier actividad malintencionada por parte del PROVEEDOR.

Una vez el servicio concluya, o el CLIENTE lo solicite anticipadamente, se hará cese de uso de la firma electrónica y de las credenciales. Lo cual además implica que la firma electrónica será eliminada de los navegadores web y computadores del PROVEEDOR.

Cláusula Sexta: Recomendación de seguridad credenciales SII.

Para el caso de la firma electrónica se recomienda autorizar a un usuario del PROVEEDOR en el SII y no enviar la firma electrónica real de un usuario del CLIENTE. Sin embargo, se debe considerar que para poder prestar el servicio la el usuario del PROVEEDOR autorizado deberá tener al menos los mismos privilegios y permisos en SII que la firma real del usuario del CLIENTE que ha solicitado el servicio.

Para el caso del RUT y clave del SII se recomienda cambiar la clave antes de entregar al PROVEEDOR, y luego volver a cambiar la clave cuando el servicio concluya. Así el CLIENTE se asegura de que no se tendrá acceso nuevamente en el futuro.

Cláusula Séptima: No confidencialidad

No habrá deber alguno de confidencialidad en los siguientes casos:

- Cuando el PROVEEDOR tenga evidencia de que conoce previamente los datos recibidos.
- Cuando los datos recibidos sean de dominio público.
- Cuando los datos dejen de ser confidenciales por ser revelados por el CLIENTE.