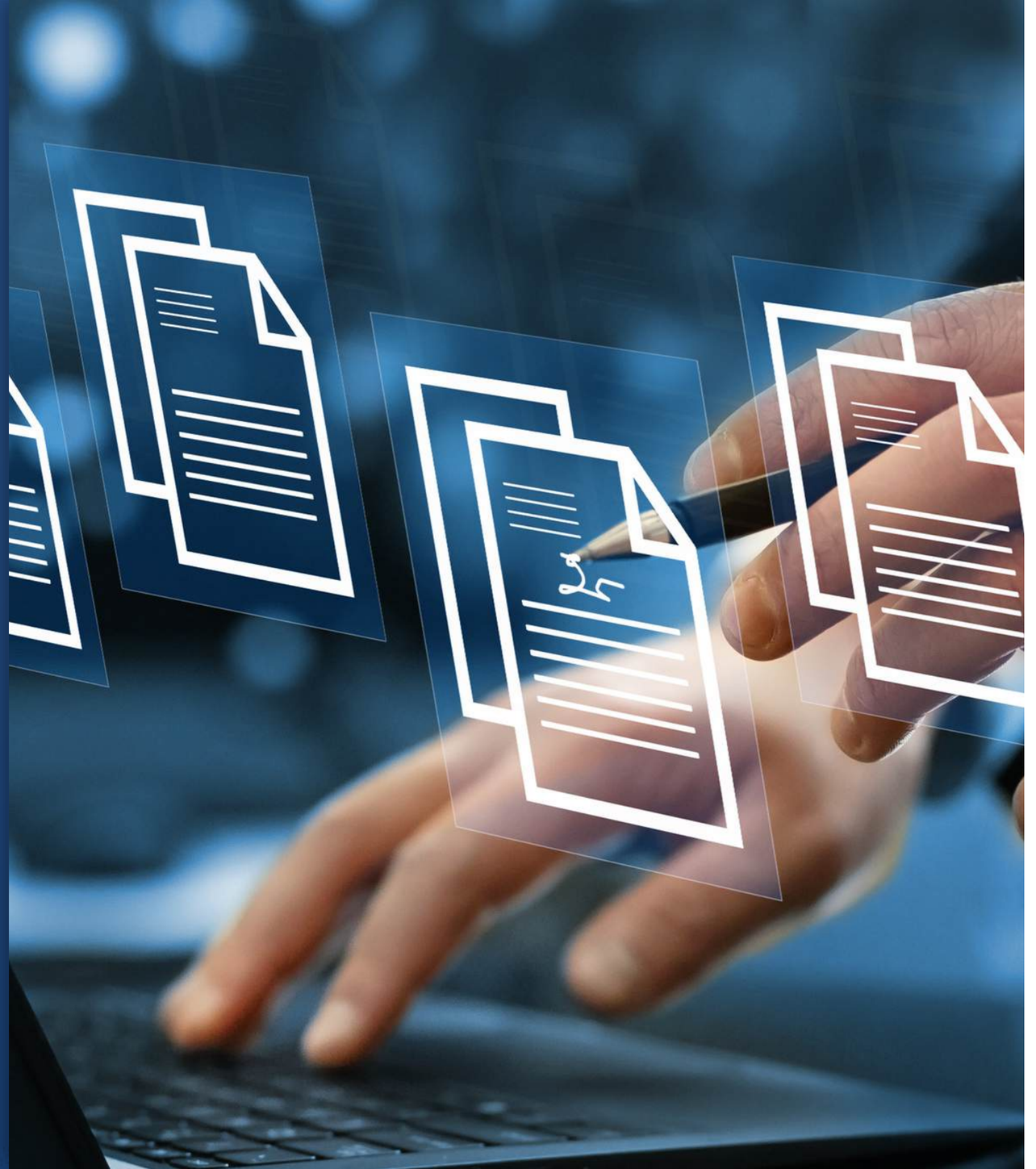
FIRMA REMOTA

TABLA DE CONTENIDO



¿QUÉ ES LA FIRMA REMOTA?

D.S. 029-2021-PCM

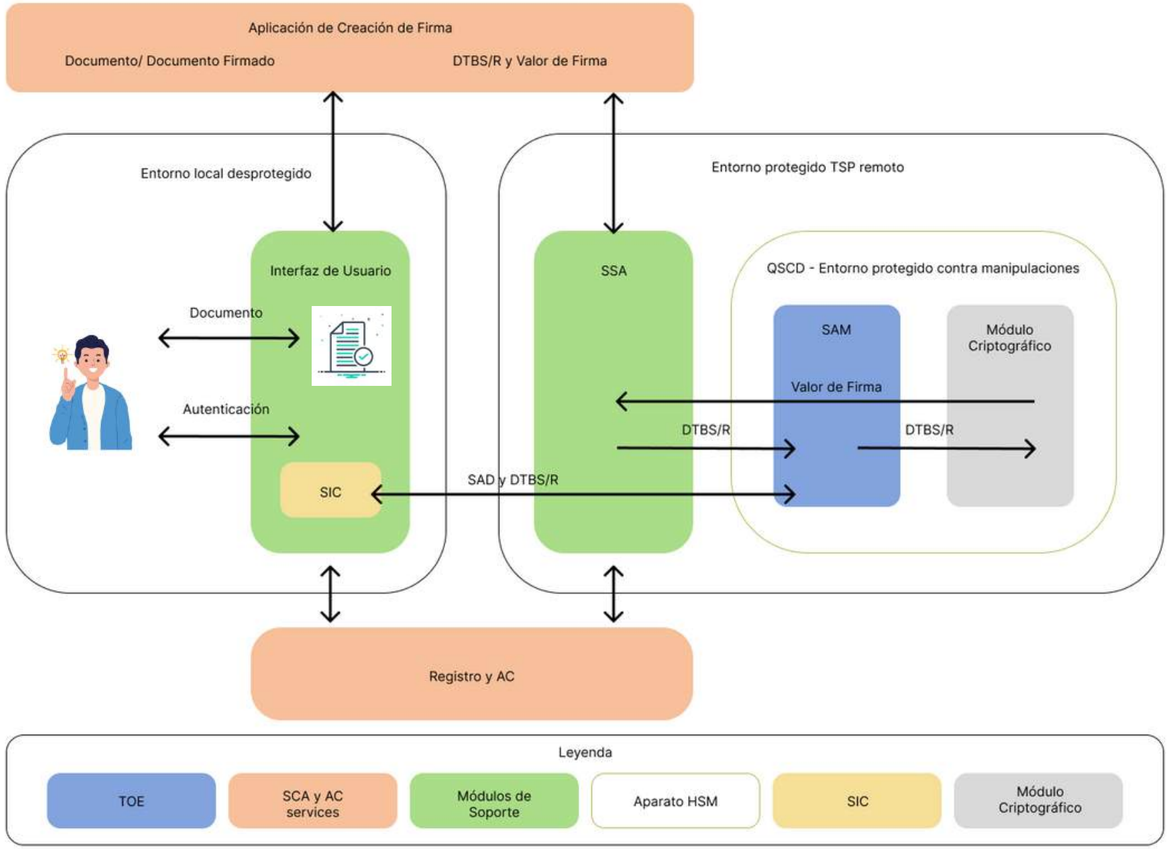
La firma remota es una modalidad de firma digital que te permite firmar documentos electrónicamente utilizando claves privadas que se encuentran almacenadas y gestionadas de forma segura por un tercero. A este tercero se le denomina Prestador de Servicios de Valor Añadido del tipo Firma Remota.

EJEMPLO 1.

Si eres un funcionario público y necesitas firmar digitalmente un expediente, pero el certificado digital asociado a tu Documento Nacional de Identidad Electrónico (DNIe) está en tu oficina, podrías utilizar un servicio de firma remota. En este caso, el "Prestador de Servicios de Valor Añadido acreditado en la modalidad de sistema de creación de firma remota" sería el encargado de gestionar de forma segura tu clave privada. Tú te autenticarías en el sistema del prestador de servicios y, a través de él, podrías aplicar tu firma digital al documento sin necesidad de tener el DNIe físicamente contigo.

¿CUÁLES SON LOS COMPONENTES DE LA FIRMA REMOTA?

VISIÓN GENERAL



ABREVIACIONES

QSCD Dispositivo de creación de firma electrónica calificada

TSP Proveedor de servicio de confianza

SAD Datos de activación de firma
Es la autenticación del firmante

SAM Módulo de activación de firma
Verifica los factores de autenticación del firmante

SSA Aplicación de firma de servidor

SAP Protocolo de activación de firma

SIC Componente de interacción del firmante

DTBS Data a ser firmada

TOE Target of evaluation, Objeto de evaluación

EN 419241-1:2018

Módulo de Activación de Firma (SAM)

Un SAM (Módulo de Activación de Firma) es un software que se asegura de que las claves de firma digital solo se usen bajo el control del firmante.

Sirve para:

- Garantizar el control exclusivo: Confirma que el suscriptor es la única persona que puede autorizar el uso de la clave de firma.
- Activar la firma: Recibe tus datos de activación de firma (SAD), que son como una confirmación del suscriptor, para permitir que se realice la operación de firma digital.
- Proteger la clave: Opera en un entorno seguro y protegido para asegurar que tus claves de firma estén siempre a salvo y se usen de forma confiable.

EN 419241-1:2018

¿Como funciona el SAM?

Cuando un suscriptor desea firmar algo, el SAM espera recibir una "confirmación". Esta confirmación se llama SAD (Datos de activación de firma). El SAD es un conjunto de datos que el firmante, genera o recolecta de forma segura, a menudo a través de un "Componente de Interacción del Firmante" (SIC).

EN 419241-2:2019

¿Cuáles son los requisitos de seguridad que debe cumplir el SAM?

1. Protección de la clave de firma: Debe asegurar que la clave que usa el suscriptor para firmar solo se active y use cuando él lo autoriza explícitamente. Es decir, ni siquiera los administradores de la solución pueden alterar o intervenir en el proceso de firma. Es como tener un control remoto muy seguro para la clave de firma.

EN 419241-2:2019

¿Cuáles son los requisitos de seguridad que debe cumplir el SAM?

2. Verificación de la autorización del Suscriptor (SAD): Cuando el suscriptor envía una señal para firmar (los Datos de Activación de Firma o SAD), el SAM tiene que verificar muy bien que esa señal es auténtica, que no ha sido suplantada, y que está ligada a lo que el suscriptor quiere firmar y a su clave específica. No debe permitir firmas si no hay una autorización clara y correcta.

EN 419241-2:2019

¿Cuáles son los requisitos de seguridad que debe cumplir el SAM?

3. Funcionamiento en un entorno seguro: El SAM debe operar en un lugar muy protegido, a prueba de manipulaciones, ya sea dentro del mismo módulo criptográfico que guarda la clave, o en un hardware dedicado y seguro. Esto evita que alguien pueda alterarlo o acceder a él sin permiso.

EN 419241-2:2019

¿Cuáles son los requisitos de seguridad que debe cumplir el SAM?

4. Resistencia a ataques: Tiene que estar diseñado para resistir intentos de suplantación o manipulación, como ataques que intenten copiar la firma del suscriptor, modificar el documento sin su permiso, o usar su clave sin que él lo sepa.

EN 419241-2:2019

¿Cuáles son los requisitos de seguridad que debe cumplir el SAM?

5. Registro de eventos: Debe llevar un registro de todas las acciones importantes relacionadas con la seguridad, como quién intentó firmar, cuándo y si se autorizó la firma, para poder auditarlo si es necesario.

EN 419241-2:2019

¿Cuáles son los requisitos de seguridad que debe cumplir el SAM?

6. Uso de criptografía fuerte: Todas las operaciones criptográficas que realice el SAM (como generar números aleatorios o proteger datos) deben usar algoritmos y claves fuertes, aprobados por autoridades reconocidas.

EN 419241-2:2019

¿Cuáles son los requisitos de seguridad que debe cumplir el SAM?

7. Comunicación segura: La comunicación entre el SAM y otros componentes (como el dispositivo desde donde se autoriza la firma o el módulo criptográfico) debe ser segura y protegida contra modificaciones o revelación.

RESOLUCIÓN 175-2025 -DGI-INDECOPI

¿Cuáles son los requistos que evaluará la IOFE?

A partir de ahora el INDECOPI evaluará el cumplimiento de una lista de requisitos de seguridad, para que un proveedor pueda ofrecer un servicio de firma remota o para que mantenga su acreditación.

Es decir, aquellos proveedores listados en la TSL, ya están prontos a recibir una evaluación de seguimiento, donde se auditará el cumplimiento de los siguientes requisitos:

RESOLUCIÓN 175-2025 -DGI-INDECOPI

¿Cuáles son los requistos que evaluará la IOFE?

1. La clave privada del firmante (suscriptor) se genera en un módulo criptográfico del proveedor del servicio.

En palabras sencillas: La "clave secreta" para firmar no se crea en la computadora personal, sino en el HSM que tiene el proveedor del servicio de firma remota.

RESOLUCIÓN 175-2025 -DGI-INDECOPI

¿Cuáles son los requistos que evaluará la IOFE?

2. La generación de claves debe hacerse solo con datos que solo el firmante conoce y controla.

- En palabras sencillas: Cuando se crea la "clave privada del suscriptor", la información que se usa para generarla debe ser algo que solo el suscriptor tiene en su poder o conoce. El proveedor no debe poder crear la clave del suscriptor por sí solo.

RESOLUCIÓN 175-2025 -DGI-INDECOPI

¿Cuáles son los requistos que evaluará la IOFE?

3. El sistema debe estar configurado para que el proveedor del servicio no pueda conocer las claves privadas de los suscriptores.

- En palabras sencillas: El proveedor del servicio de firma, ni sus empleados, ni sus sistemas, deben poder "ver" o "saber" cuál es la clave privada. No pueden acceder a ella directamente, ni verla en los registros de operaciones, ni aprovecharse de alguna falla del sistema para descubrirla.

RESOLUCIÓN 175-2025 -DGI-INDECOPI

¿Cuáles son los requistos que evaluará la IOFE?

4. El dispositivo de creación de claves del proveedor debe ser diferente e independiente al dispositivo de la entidad que emite tu certificado digital.

- En palabras sencillas: El dispositivo donde se crea la clave y se gestiona la firma no debe ser el mismo que usa la autoridad que emitió el certificado digital (tu "identificación digital"). Son sistemas separados para mayor seguridad.

RESOLUCIÓN 175-2025 -DGI-INDECOPI

¿Cuáles son los requistos que evaluará la IOFE?

5. El proveedor debe tener un sitio principal y uno de respaldo (contingencia) para asegurar que el servicio de firma siempre funcione.

- En palabras sencillas: Para que siempre puedas firmar, el proveedor debe tener dos instalaciones: una principal y otra de emergencia, por si la primera falla. Ambas deben tener su propio "HSM" para crear firmas remotas. Se verificarán con visitas presenciales, a menos que ya tengan certificaciones de estándares reconocidos.

RESOLUCIÓN 175-2025 -DGI-INDECOPI

6. Se deben cumplir las siguientes especificaciones adicionales:

- a) El dispositivo de firma (HSM) debe tener una certificación específica (CEN-EN 419.221, parte 5) o equivalente.
- b) Antes de firmar, el sistema pedirá al suscriptor autenticarse con múltiples factores (OTP, biometría, etc.).
- c) El sistema debe registrar evidencias de la firma y garantizar que el suscriptor tiene el control exclusivo sobre ella.
- d) Antes de firmar, el sistema te debe mostrar los datos a firmar de forma clara y sin posibilidad de manipulación.

RESOLUCIÓN 175-2025 -DGI-INDECOPI

- e) El sistema debe ser resistente a ataques informáticos y usar canales seguros de comunicación.

RESOLUCIÓN 175-2025 -DGI-INDECOPI - PRECISIONES ADICIONALES

- Si los evaluadores necesitan más información para verificar si un proveedor cumple con los requisitos del primer acápite, pueden usar como guía otros estándares técnicos importantes, como el CEN EN 419.241 (parte 1 y 2) o el ETSI TS 119.431 (parte 1 y 2) y el ETSI TS 119.432.

RESOLUCIÓN 175-2025 -DGI-INDECOPI - PRECISIONES ADICIONALES

- Además de todo lo que dice esta resolución, los proveedores de servicios de firma remota también deben cumplir con otros requisitos generales que apliquen de la "Guía de Acreditación de Servicios de Valor Añadido".
  - por ejemplo, el uso de sello de tiempo, la cobertura de un Sistema de Gestión de la Seguridad de la Información, la certificación ISO 27001:2022.

RESOLUCIÓN 175-2025 -DGI-INDECOPI - PRECISIONES ADICIONALES

Cuando un proveedor solicite su acreditación (o renovación), debe explicar detalladamente cómo va a cumplir con cada uno de los requisitos establecidos en esta resolución.

Es decir debe presentar evidencias: configuraciones en el HSM, seguridad del SAM, protección del SAM por un entorno hardware seguro.

RESOLUCIÓN 175-2025 -DGI-INDECOPI - PRECISIONES ADICIONALES

- La emisión del certificado digital y la verificación de la identidad del suscriptor son trabajo de la "Entidad de Certificación" y la "Entidad de Registro".
- Además, la Entidad de Certificación debe actualizar sus documentos (Políticas de Certificación y Declaración de Prácticas de Certificación) para incluir el tipo de certificado digital que se usa para la firma remota. La Entidad de Registro también tiene la misma obligación.

RESOLUCIÓN 175-2025 -DGI-INDECOPI - PRECISIONES ADICIONALES

- El software que usa el proveedor para realizar la firma remota (el "motor de firma") debe ser acreditado, es decir, debe pasar por un proceso de acreditación para mostrar que es seguro y funciona correctamente.
- Además, la aplicación que usa firmante (en su celular o computadora) para pedir la firma remota y dar tus datos de identificación, también tendrá que pasar por un proceso de acreditación del tipo "Sistema de Intermediación Digital".

RESOLUCIÓN 175-2025 -DGI-INDECOPI - PRECISIONES ADICIONALES

Si en la primera auditoría anual de supervisión se encuentran problemas o hallazgos, el proveedor acreditado tiene la opción de pausar la auditoría por tres meses para arreglar esos problemas antes de que continúe la evaluación.

RESOLUCIÓN 175-2025 -DGI-INDECOPI - PRECISIONES ADICIONALES

En lugar de pasar por todas las auditorías locales detalladas en los acápites anteriores, los proveedores pueden presentar certificaciones de cumplimiento de estándares internacionales reconocidos, como ambas partes del CEN EN 419.241 o las normas ETSI TS 119.431 y 119.432. Esto puede simplificar el proceso de acreditación o renovación.