

CÓMO CUSTODIAR EL CERTIFICADO DIGITAL DE UN CLIENTE DE FORMA SEGURA Y LEGAL

En Firma Original ayudamos a los despachos profesionales a eliminar los riesgos asociados a la custodia y uso de certificados digitales de clientes, cumpliendo estrictamente con la normativa y manteniendo una operativa ágil y sencilla.

La custodia tradicional de certificados, instalados en ordenadores, servidores o carpetas compartidas, representa hoy uno de los mayores riesgos legales y reputacionales para asesores, gestores, y todos los despachos profesionales.

La mala praxis más extendida

Actualmente es una práctica de lo más habitual que el asesor tenga instalados, en su ordenador, los certificados de sus clientes. O que los certificados digitales se guarden en un servidor o carpeta compartida, accesible por todo el personal del despacho, y que sean instalados localmente cuando se requiera realizar un trámite con ellos.

La sugerencia, y lo que indica la norma, es que cada uno tenga control de su certificado y que no lo ceda a nadie. Pero la realidad es que los despachos asumen más responsabilidad de la que deberían, y los clientes menos de la que les toca.

Pocos despachos tienen consciencia del **riesgo** que corren con esta práctica.

Pocos clientes, titulares de los certificados, son conscientes del **riesgo** que asumen cuando su asesor sigue esta práctica.



El 85% de despachos no cumple la seguridad mínima.

Qué riesgos conlleva ceder el certificado a un tercero

El certificado digital permite a su titular, entre otras cosas, lo siguiente:

- Identificarse frente a Organismos Públicos y también Privados, como las entidades financieras.
- Tramitar de forma oficial con entidades públicas y privadas, para la presentación de impuestos, subvenciones, licitaciones, y la realización de pagos o transferencias.
- Firmar documentos legalmente, como contratos, actas, cuentas, consentimientos.

¿Qué pasa si NO es el titular quien está utilizando el certificado?

Aunque el uso del certificado por parte de una persona distinta al titular (o por un proceso automatizado) sea lícito e incluso ético, le llamamos “usurpación de identidad” o “fraude de identidad”. Partiendo de que el certificado es personal e intransferible, toda cesión de uso podría considerarse una pérdida de control del certificado por parte de su titular.

Y, obviamente, esta persona o proceso automatizado puede realizar las acciones relacionadas haciéndose pasar por el titular del certificado. Para lo bueno y para lo malo.

El **riesgo** para el titular es extremo, ya que estas acciones pueden derivar en fraudes, delitos, facturas falsas, contratos firmados sin autorización, operaciones contrarias al interés particular o colectivo, y todo lo que podamos imaginar dentro del mundo de la tramitación electrónica. Y será el titular quien formalmente estará realizándolo.

Qué riesgos tiene usar el certificado de un cliente

La responsabilidad que tiene el despacho, y sus profesionales, al usar el certificado de un cliente es muy alta. Y si añadimos que se custodia el certificado del cliente en los ordenadores del despacho, esta responsabilidad se dispara igual que la posibilidad de que ocurra un incidente.

Quién no ha padecido u oído alguno de los casos siguientes:

- Robo de información por un ataque informático, con los certificados expuestos como el resto de los documentos.
- Incidente con personal resentido que actúa de mala fe, pudiendo acceder sin autorización ni control a (y por tanto usar) los certificados de los clientes a los que ya no debería tener acceso.
- Pérdida de los certificados de los clientes instalados localmente en los ordenadores del despacho, por fallos en los dispositivos o por cambios técnicos.
- Y, últimamente también empieza a verse, la denuncia de un cliente al despacho por uso no autorizado ni consentido de su certificado digital.

El **riesgo** para el despacho, y sus profesionales, puede llegar a niveles reputacionales e incluso legales. Una pérdida de confianza por parte de los clientes, derivada de un fallo de seguridad o de operativa, puede ser desastrosa. Un incidente de Protección de Datos, considerando el certificado como un dato personal sensible, puede conllevar una sanción. Y una denuncia por usurpación de identidad derivada de una mala praxis, puede conllevar la complicidad en un delito grave.

La solución de custodia segura y legal

El objetivo de todo despacho, en relación con los certificados de sus clientes, debe ser minimizar riesgos para todas las partes, al tiempo que desarrolla las tareas encomendadas.

Básicamente, lo que necesita el despacho son tres cosas:

1. Custodiar de forma **segura** y con control de acceso los certificados de sus clientes.
2. Que la custodia y el uso de cada certificado sea **legal**, estando autorizada explícitamente por el correspondiente cliente, titular del certificado digital.
3. Que la operativa del día a día con los certificados digitales sea **cómoda** y eficiente.

Existen en el mercado varias, no muchas, herramientas que permiten al despacho cubrir los anteriores requerimientos. Algunas cubren uno o dos puntos, y pocas cubren los tres.

Con nuestra solución tenemos cubiertos los tres requerimientos, y se fundamenta en las siguientes funcionalidades:

- a. La custodia se realiza en la nube, propia, securizada, con control de acceso para cada usuario autorizado. Al estar en la nube, los certificados no se pierden ni se borran. El almacenamiento de los certificados se realiza de forma que no pueden exportarse, ni se conocen las claves ni contraseñas, por parte de ningún usuario.
- b. Tanto la custodia y el uso del certificado, por parte del despacho, quedan autorizados explícitamente por su titular, mediante la firma electrónica del correspondiente documento, que queda almacenado en el propio sistema disponible para futuras auditorías que lo pudieran requerir.
- c. No es necesario entonces mantener los certificados instalados en cada ordenador. Los usuarios habilitados accederán a la lista de los certificados que tengan autorizados, y activarán / desactivarán cómodamente sólo los que deseen tener visibles en cada momento en su ordenador. La operativa del usuario es idéntica a la que tiene con los certificados instalados en su ordenador, sólo que no puede “llevárselos” y sólo accede a los que tiene autorizados.

Confiamos en que este texto ayude a la concienciación tanto de los despachos, con sus profesionales, como también a los titulares de los certificados digitales, en la gestión y custodia de los mismos, eliminando, o como mínimo minimizando, los riesgos.