

LO QUE NADIE ESTÁ DICIENDO SOBRE LA NUEVA E.FIRMA PARA EL IMSS

Si bien el acuerdo publicado por el H. Consejo Técnico del IMSS, mediante el cual la **e.firma del SAT se convierte en el único certificado digital válido para los movimientos afiliatorios y la vinculación de representantes legales**, ha sido presentado como una medida de simplificación administrativa; hay aspectos de suma relevancia que van más allá de un cambio tecnológico y no se está hablando de ello.

Durante más de veinte años el sistema de certificados digitales tenía la característica de que era la **identidad digital administrada por el propio IMSS** y con esta adecuación ahora la identidad digital deja de pertenecer a esta institución y **pasa a depender del sistema nacional administrado por el SAT** mediante la e.firma y esto significa que la autenticación deja de ser sectorial y se convierte en una identidad única para interactuar con diversas autoridades.

Adicionalmente, durante lo que va del 2026 el Gobierno Federal ha impulsado diversos acuerdos de simplificación administrativa y digitalización que buscan integrar **trámites mediante plataformas que operan de forma transversal**, además de reducir requisitos y fortalecer la identificación electrónica. Ahora bien, esto, supuestamente genera una mayor certeza pues cada movimiento quedará vinculado a una persona perfectamente identificada, es decir, **se pretende** que deje de existir duda sobre quién realizó un alta, una baja o una modificación salarial y con ello la **trazabilidad sea prácticamente absoluta**.

Este cambio por parte de la Institución significa que cuando un representante legal ya no trabaja en la empresa, ya no se podría seguir autenticando como pasaba con los certificados digitales que permanecían activos. Además, se dejará de mantener una infraestructura propia de emisión, renovación y validación de certificados que representa costos elevados al dejar de administrar ese ecosistema y aprovechar una infraestructura nacional ya consolidada. No menos importante sería pensar que **la autoridad podrá validar con mayor facilidad información** proveniente de diversas autoridades como el SAT, del Registro Público, del RFC y de otras bases gubernamentales **por los convenios de intercambio de información** que sin duda serán más eficientes. Pero de todo esto, la pregunta importante es:

¿la e.firma realmente identifica quién realizó un trámite?

Uno de los principales argumentos para sustituir el certificado digital del IMSS por la e.firma del SAT es fortalecer la identidad digital y brindar mayor seguridad jurídica, y sí, en teoría cada trámite quedará asociado a una persona plenamente identificada. Sin embargo, cuando trasladamos esa idea a la operación cotidiana de las empresas, **una cosa es identificar al titular de una firma electrónica y otra muy distinta identificar a la persona que realmente ejecutó el movimiento**.

En la operación cotidiana de una empresa, **resulta casi imposible que el representante legal sea quien, de manera personal, ingrese a las plataformas gubernamentales** para realizar los trámites electrónicos. Aunque jurídicamente es la persona facultada para representar a la empresa frente a las autoridades, la ejecución material de estas obligaciones suele recaer en las áreas especializadas de Recursos Humanos, Nóminas, Seguridad Social, Fiscal, Contabilidad o Jurídico, e incluso en consultores externos o despachos especializados contratados para tal efecto. Son estos profesionales quienes preparan la información, capturan los datos y presentan movimientos afiliatorios, dictámenes a través de SIDEIMSS, solicitudes de registro patronal, avisos de SIROC, declaraciones de ICSOE y SISUB, trámites relacionados con REPSE, aclaraciones, devoluciones y una amplia gama de gestiones indispensables **para el cumplimiento de las obligaciones patronales.**

En este contexto, **la intervención del representante legal generalmente se limita a otorgar la autorización para que dichos trámites se lleven a cabo o a poner a disposición su e.firma para su presentación**, sin que ello implique que participe directamente en la elaboración, revisión o envío de cada gestión. Esta realidad operativa plantea un desafío importante para el nuevo modelo de autenticación porque, aunque la e.firma identifica al titular del certificado utilizado, no necesariamente acredita quién realizó materialmente el trámite desde la computadora, quién capturó la información o quién decidió enviarla. Por ello, **el verdadero reto no radica únicamente en la autenticación tecnológica, sino en la implementación de controles internos que permitan documentar, con trazabilidad** suficiente que determine qué persona utilizó la e.firma, bajo qué autorización y para la ejecución de qué procedimiento específicamente.

¿Qué deberían hacer los patrones?

Cabe señalar que la e.firma es la llave maestra, sin embargo, la siguen utilizando como un archivo más. Ante la transición se presenta una oportunidad para **profesionalizar la administración de la identidad digital** corporativa pues cabe señalar que la e.firma es un activo estratégico que debe administrarse con el mismo control que las cuentas bancarias, los sellos digitales o las claves de acceso a sistemas críticos de la empresa.

Es importante que no todas las personas necesitan conocer la contraseña, por el contrario, **debe existir un número reducido de custodios autorizados**, sobre todo, quienes realmente operan el sistema. Para ello, se puede implementar un registro de utilización para fortalecer la trazabilidad, que contenga:

- fecha;
- hora;
- trámite realizado;
- responsable operativo;
- autorización correspondiente

¿Qué falta?

Este cambio también abre la puerta a un debate que probablemente veremos en los próximos años pues es indispensable evolucionar hacia **esquemas de firma electrónica delegada, autenticación multifactor o gestión de identidades empresariales**, donde el representante legal conserve la titularidad jurídica de la e.firma, pero los actos operativos queden vinculados a usuarios autorizados con trazabilidad individual.

En otros países, sobre todo de la **Unión Europea**, los sistemas de administración pública y plataformas corporativas ya utilizan modelos de Identity and Access Management (IAM), registros de auditoría (logs), autenticación multifactor (MFA) y segregación de funciones para **distinguir entre quien ostenta la representación legal y quien ejecuta materialmente un trámite**. En México, la generalización de la e.firma como llave única para interactuar con diversas autoridades podría impulsar, en el mediano plazo, una evolución normativa y tecnológica en ese mismo sentido.

Entonces, **la solución es crear un modelo más robusto de gestión de identidades digitales**, pues así las empresas ya no tendrían que compartir la e.firma del representante legal para cumplir con sus obligaciones cotidianas. Cada colaborador o asesor accedería con sus propias credenciales, dentro de las facultades previamente autorizadas, mientras el sistema conservaría evidencia completa de quién realizó cada trámite, cuándo lo hizo y bajo qué autorización. Ese modelo fortalecería simultáneamente la seguridad jurídica, la ciberseguridad y el gobierno corporativo, **reduciendo uno de los principales riesgos que hoy enfrentan las organizaciones en la administración de su identidad digital**.

¿Compliance digital?

La adopción de la e.firma como mecanismo de autenticación único no debe analizarse únicamente desde la óptica de un trámite administrativo, sino como parte de una **transformación que involucra la gestión integral de riesgos, protección de la información y cumplimiento normativo**. Es por ello por lo que el compliance digital será necesario para diseñar políticas de custodia de la e.firma, implementar esquemas de segregación de funciones, mantener bitácoras de uso, fortalecer la autenticación mediante mecanismos adicionales cuando sea posible, controlar los accesos conforme al principio de mínimo privilegio, realizar auditorías periódicas, definir protocolos para la renovación, revocación y resguardo de las credenciales digitales, en otras palabras, la gestión **de la identidad electrónica debe incorporarse a los programas de cumplimiento para evitar riesgos de fraudes**.
