Un tema relevante que no se le ha dado la suficiente importancia: cuidado de las claves en el SII

Estimados(as):

Quisiera llamar la atención sobre un tema que es relevante y que a veces no se le da la importancia que ello requiere: **el cuidado de la administración de las claves de acceso al sistema informático del SII** (también esto aplica para todo, ya que hoy las operaciones bancarias, de remuneraciones, de órdenes de compra, inversión etc., funcionan en plataformas en las cuales se utiliza el acceso vía claves).

Hasta el momento, la empresa es el contribuyente que vía la actuación de su representante legal, obtiene el acceso a la plataforma informática del SII, que permite varias acciones como el conocer todo el historial (declaraciones e información asociada al RUT de la empresa), y también el realizar todos los trámites permitidos vía electrónica (autorizar documentos electrónicos como facturas, notas de crédito, débito, boletas, etc., como también emitir dichos documentos y la presentación de modificaciones de representantes legales, declaraciones y otros trámites).

Este administrador tiene la potestad de entregar autorización para que otras personas realicen alguno de los trámites, entregando facultades parciales o totales. Por ello, hay instancias en que el acceso total es compartido para otras personas que son autorizadas para realizar ciertas acciones, las cuales una vez desarrolladas son notificadas vía correo a un destinatario que se supone "son los ojos del administrador", para notificarse que han realizado acciones en la plataforma. Por ello, es vital saber quién está informado de lo que está pasando en el RUT de la empresa, por acciones de todos los usuarios autorizados para realizar algún trámite o acción en la plataforma.

Dado que lo anterior es casi imposible dejarlo en una sola persona, dependiendo del tamaño de la empresa, muchas veces hay poca rigurosidad en el cuidado de los protocolos para asignar los roles de los distintos usuarios que realizan proceso que se asocian a la empresa. Por ejemplo, si inicialmente es el representante legal el que tiene acceso a la clave de administrador, éste la comparte o se la entrega a su contador, luego éste se la deriva al ayudante para que opere en el RUT de la empresa. Así, puede que los procesos sean realizados con la misma clave, sin tener conciencia de que hay una posibilidad de delegar parte de la función matriz que es la representación legal y la respectiva responsabilidad que le compete al representante legal de la empresa.

También, como lo pueden ver en la siguiente situación publicada días atrás, Reportaje Bío Bío, pueden existir procesos de mal uso de la plataforma del SII, a través de engaños más atrevidos y sofisticados como la suplantación de representación legal para modificar la clave de acceso y así operar fraudulentamente.

Lean el artículo y pueden desde ya ir tomando conciencia de lo relevante que es y seguirá siendo el tomar el control de la administración de la clave, que prontamente debería ser "clave única", por persona, para así dejar establecido un proceso más amplio de delegación donde cada actuante tenga el perfil parcial asociado a la "clave única" y ella no sea compartida sin conocer la responsabilidad que existe de entregar esa información a un

tercero (por ejemplo, si hoy soy un trabajador de una empresa y actuó con la clave que está a nombre del dueño de la empresa, es de éste la responsabilidad de mis actos, dado que no estoy actuando con mi clave personal).

Otra cosa relevante es conocer cuál es el "correo de contacto" con el SII, para que el sistema se comunique con la empresa (RUT) cuando existan actuaciones como lo que comenta el reportaje. Si dicho correo no es revisado constantemente, aunque es ideal que esté el línea (quizás el mismo SII debiera agilizar una forma de comunicación vía telefónica, vía mensaje a más de un correo o persona, para que así también se tengan un proceso de alerta que pueda evitar el mal uso de procesos informáticos no deseados).

Nosotros como asesores también tenemos responsabilidad de cuidar el proceso y así lo hacemos, en especial buscando cuidar el uso adecuado de las escalas de permisos que la plataforma permite, pero claramente es el contribuyente directamente el que debe tomar conciencia de su exposición, más aún que se sigue privilegiando la actuación on line, lo que deriva en una necesidad de operación 24/7 que hay que acostumbrase a administrar (los malos no descansan).

Saludos,

OMAR A. REYES RÍOS
Ricardo Lyon 222, Of 703, Providencia
Fono: +56 222 701 000 • ww.circuloverde.cl