https://transformacionpublica.cl/

# ***Transcripción Coloquio de Transformación Digital: Autenticación y uso de firma electrónica avanzada en el sector público chileno***

## *06.11.2020*

-José Inostroza: (00:44) Buenos días, estamos ya en esta tradicional maratón de coloquios en transformación pública, ya casi un coloquio por semana, lo cual habla del interés que tenemos todos en esta comunidad de estos temas, pese a todo lo complejo que puede estar el contexto en el país y a nivel internacional. Seguimos hablando de transformación digital en el Estado, porque nos entusiasma mucho y sabemos que es muy importante. Estamos en Zoom y vía YouTube

En esta ocasión tenemos un invitado de lujo, lo digo porque ya no sólo a estas alturas nos une una cierta amistad con Renato, sino porque efectivamente es muy reconocido. Es una de las personas que más sabe probablemente de Derecho informático en el país, tiene una larguísima trayectoria en esta materia y en esta ocasión nos va a ayudar con el tema de la autenticación, tal vez identidad digital. Él nos podría eventualmente hacer una distinción entre esos dos conceptos, si es que existe. Y lo más importante, en la firma electrónica avanzada. Esto es de una relevancia mayor para los que no saben, porque ahora, de aquí en adelante, todos los procedimientos administrativos van a ser completamente electrónicos. Es fundamental tener certeza de que la persona que está al otro lado de la pantalla, ya sea un ciudadano, una autoridad o un funcionario, sea efectivamente la persona que tiene que ser y tener las competencias que corresponde. Y que su expresión de voluntad en distintos documentos también tenga el mayor nivel de certeza jurídica o la que corresponda en cada ocasión. Y para eso tenemos un sistema ya hace tiempo, no reciente, sobre documento electrónico y firma electrónica, tema sobre el cual Renato escribió un libro, de la editorial Andrés Bello, lo cual denota la importancia de los conocimientos de Renato. El libro se denomina “Comercio electrónico, firma digital y derecho: Análisis de la Ley 19.799”

(02:47) Voy a hacer algunas referencias rápidamente sobre el currículum de Renato. Él es abogado y profesor de Derecho Informático de la Universidad Católica de Valparaíso, que es una unidad académica que ha sido especialmente activa en la comunidad nacional en estas materias y ha realizado algunos seminarios recientemente, ha hecho un gran aporte. Y no sólo es profesor, sino que además es asesor jurídico en temas tecnológicos, en probablemente la institución más sofisticada en esta materia, el Servicio de Impuestos

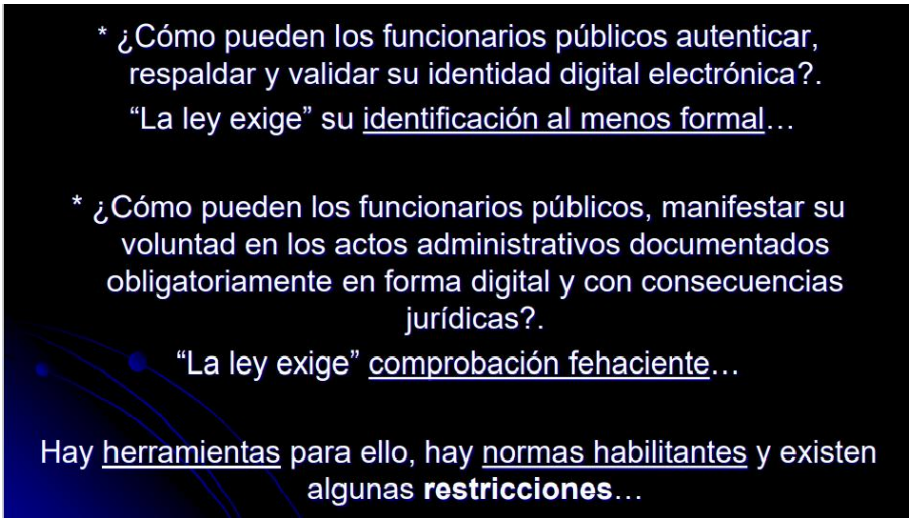
Internos, donde lleva ya 19 años ejerciendo como asesor y especialista, lo cual obviamente nos da mucha confianza a todos nosotros.

También en el pasado fue director del Centro de estudios de Derecho Informático de la Universidad de Chile, y profesor del Magíster de Derecho y Tecnología de la misma universidad. Y además el 2008, por un año y algo, fue asesor legal de la secretaría ejecutiva del grupo de Estrategia Digital del Gobierno de Chile. Tiene un Magíster en Derecho Público en la Universidad Católica de Valparaíso, además un Magíster en Gobierno Electrónico de la Universidad Tecnológica Metropolitana y un Diplomado en Derecho Informático de la Universidad de Zaragoza, como pueden apreciar, claramente, Renato tiene una trayectoria larguísima y muy consistente en esta materia, y eso, como dije, es ampliamente reconocido. Renato, te agradecemos que estés con nosotros en esta ocasión, y te señalamos que tienes entre 40 a 50 minutos para hacer tu presentación y después vamos a tener una conversación de también unos 50 minutos con la comunidad. Tienes la palabra.

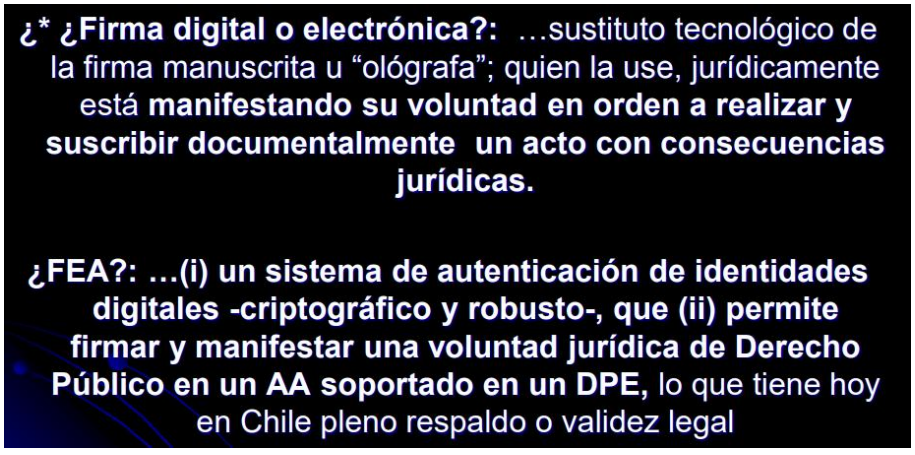
-Renato Jijena: (04:53) Gracias a ti y a tu equipo de trabajo. Es tremendamente interesante juntarse una mañana de viernes a conversar de estos temas desde una perspectiva legal, pero también desde una perspectiva de implementación real de los desarrollos tecnológicos.


He visto que ustedes han avanzado en este tema hasta la fecha, me parece extraordinariamente relevante que hayan escogido este tema de la autenticación de los elementos electrónicos, en concreto un mecanismo robusto y criptográfico.

Me parece ahora muy importante aclararlo, porque voy a decirlo al inicio, es como mi hipótesis de trabajo que quiero compartirles antes de la conversación, dice ahí: "Estado del Arte". Yo creo que si hay algo que está bien en este minuto, de cara a la implementación de procedimientos administrativos electrónicos que se nos viene en Chile, sean los grandes procedimientos, los grandes servicios, o los servicios más pequeños, es el tema de la autenticación vía firma electrónica. Hoy en día existen herramientas, existen normas habilitantes. Hay algunas restricciones que las vamos a poner arriba de la mesa, son restricciones normativas. Pero si hay algo que está, en este minuto, como un aporte que no puede ser objeto de cuestionamiento, ni de blindaje legal, y que tiene desarrollos tecnológicos, es la posibilidad de autenticarse y firmarse. Eso es lo que genera la firma electrónica avanzada mediante PKI (Infraestructura de claves públicas) y mediante certificados digitales, así que feliz de estar conversando con ustedes esta mañana.




(06:34) Dos preguntas o dos hipótesis de trabajo que hay que intentar despejar. La primera, preguntarse: ¿cómo puede un funcionario público, estamos en el contexto de la administración del Estado, de los órganos del Estado, autenticar, respaldar y validar su identidad digital electrónica? Es decir, las credenciales con las cuales se presenta un sistema, golpea y dice: "quiero entrar, quiero interactuar con otros servicios públicos o con los ciudadanos". Y la otra pregunta, que quiero intentar despejar o aportar elementos normativos y técnicos para despejar, es: con la esencia de la firma electrónica y esto no hay que olvidarlo, ¿cómo manifiesta su voluntad esa firma, en un acto administrativo concreto, que ahora está documentado, en forma obligatoria soportado en forma digital y con consecuencias jurídicas?, ¿cómo pueden lograr estos dos grandes objetivos? Como les dije, hay herramientas para ello, hay normas habilitantes y hay algunas restricciones que se pueden levantar, o que se pueden abordar, que son restricciones legales. En concreto, todos los funcionarios públicos, cuando se enfrentan a firmar instrumentos públicos electrónicos, sí o sí, por exigencia legal, artículo cuarto ley de Firma Electrónica, tienen que hacerlo mediante firma avanzada, es decir, con certificado digital. Y esa es una barrera de entrada, es un supuesto base que hay que siempre tener presente.



Despejemos algunos conceptos antes de llegar a lo que nos convoca. Ojalá pudieran los que están conectados bajar la Ley 19.799 de Firma Electrónica, visualizar desde ya el título segundo. Ese es nuestro objetivo, ese es nuestro norte, ese es el campo normativo que blinda y especifica cómo debe implementarse cualquier proceso de autenticación electrónica de documentos.

Entonces, dos conceptos básicos y qué significan, para no marearse, porque cuando uno está en reuniones de trabajo surgen estas preguntas y es importante entenderlo. Si hablamos de **firma electrónica**, que es un concepto genérico, o **digital**, que se refiere a la pictografía simétrica a los certificados digitales, simplemente, ¿qué mecanismos de los existentes en el mercado, que son muchos, permiten manifestar voluntad para realizar un acto administrativo, en este caso, soportarlo, almacenarlo en un expediente e intercambiarlo mediante plataformas, produciendo consecuencias jurídicas de cara a los ciudadanos? Eso es una firma electrónica.

(09:10) Existe otro término ya instalado en el léxico que es la **Firma Electrónica Avanzada**. El mismo efecto, la misma manifestación de voluntad, pero usando quizás el único o el mejor sistema de autentificación, el más robusto, que es el criptográfico. Me va a permitir, y lo vamos a ver en un par de ejemplos prácticos, ahora de inicio, antes de seguir avanzando en el relato. Me permite identificarme al momento de firmar, o a un funcionario en representación de un servicio público, y me permite además manifestar voluntad. Pero con tres consecuencias técnicas que en Chile tienen reconocimiento legal: que lo dicho, lo soportado en el documento electrónico, sea íntegro, no alterado, auténtico y no repudiable, o no desconocible por el funcionario público, una vez que, por ejemplo, notificó una resolución a un ciudadano. El ciudadano está cubierto por estos tres efectos jurídicos. Tiene una doble cara: al funcionario le permite actuar de manera técnica, de manera jurídica e idónea, y el ciudadano que recibe el documento electrónico o la concesión del permiso, la notificación, la aplicación de la multa, lo que sea, tener respaldo de que no se va a desconocer lo que el acto administrativo soportado en este documento le hizo llegar.


Un par de ejemplos, a propósito de autenticación. Y esto lo digo con una cuota de orgullo: el sistema más robusto de autenticación técnica, es el que tiene implementado Impuestos Internos. Y ¿por qué? Porque cualquier contribuyente puede conectarse al servicio usando su clave tributaria, puede elegir usar la Clave Única, o puede elegir autenticarse usando su Certificado Digital. , Es decir, el mismo programa que permite manifestar voluntad y hacer un cierre de integridad de autenticación y no repudio de un documento, sirve también como elemento de autenticación, y esto se admite.

Este tipo de desarrollo está disponible hace bastante tiempo y cualquier servicio público lo puede usar. Entonces el tema del mecanismo de autenticación electrónica para respaldar identidad, está resuelto.

¿Dónde viene lo interesante? De que este mismo mecanismo en la ley vigente puede encajar dentro de lo que se denomina firma electrónica simple, que no es una definición legal, que no está en la ley ¿Por qué? Porque yo voy a entrar al sitio SII y voy a aceptar, por ejemplo, mi declaración anual de renta, o voy a entrar y voy a emitir una boleta honorario electrónica. No la firmo con certificados digitales, pero el hecho de haberme autenticado de forma idónea y estar dentro del sistema, significa jurídicamente, se entiende por asociación, esa es una definición que vamos a revisar, que todo lo que yo haga una vez autenticado, constituye una manifestación de identidad jurídica. Y eso es una consecuencia del Derecho. Los mecanismos de autentificación están disponibles en el mercado y los puede desarrollar cualquier servicio.


SERVICIO DE REGISTRO CIVIL E IDENTIFICACIÓN

REPUBLICA DE CHILE

CERTIFICADO DE MATRIMONIO

Circunscripción : SUECIA
Nro. inscripción : 440 Registro : Año : 1944
Nombre del Marido : n. N.
R.U.N. : 3.890.477-9
Fecha nacimiento : 8 Septiembre 1937
Nombre de la Mujer : N.
R.U.N. : 4.970.506-9
Fecha nacimiento : 15 Septiembre 1942
FECHA CELEBRACION : 11 Abril 1944 A LAS 09:40 HORAS.

8 Octubre 2015, 18:02.

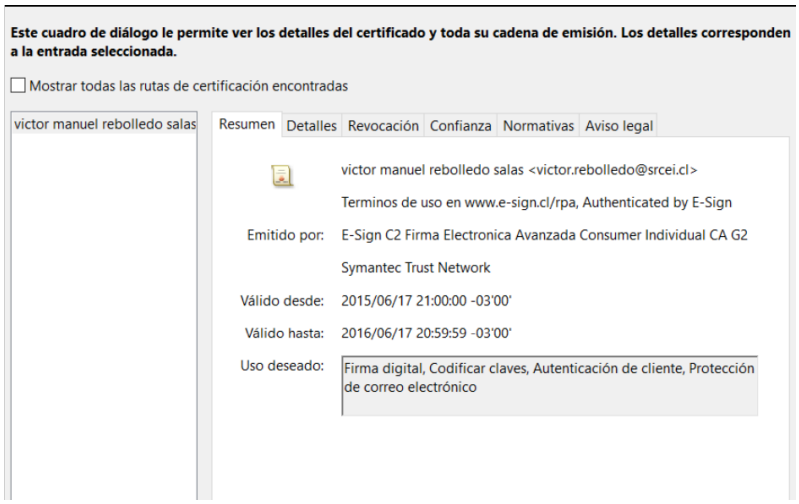
Timbre electrónico SRCeI

Víctor Rebolledo Salas
Jefe de Archivo General (S)
Incorpora Firma Electrónica Avanzada

(12:06) Pero lo que nos convoca, lo más interesante, es la llamada Firma Electrónica Avanzada. Para aquellos que están conectados y no son usuarios de Firma Electrónica Avanzada, o no manejan la bajada tecnológica concreta, aquí tenemos un instrumento público por antonomasia, un Certificado de Matrimonio emitido por el Servicio de Registro Civil. Lo interesante que hay que entender, a propósito de Firma Electrónica Avanzada, es que este documento me habla. Este documento tiene información criptográfica añadida, el llamado software digital que es un software de firma. Y yo le puedo preguntar o decir al documento: “identifícate conmigo”. Y, ¿Qué me está diciendo?

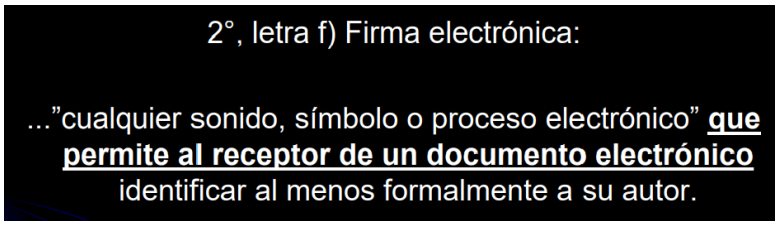
Primero, en el borde superior derecho me da un folio y un código de verificación, que es una exigencia legal del artículo 45 del Reglamento de la Ley 19.799, que dice que cada vez que se va a imprimir un documento o generar una copia, generar un segundo ejemplar, tiene que autenticarse. Y me dice que con estos números puedo ir a un sitio web del Servicio del Registro Civil e identificar este documento como válido frente a su original electrónico. Me dice además, y esto es cultural, con un timbre de agua, “esto es del Registro Civil”. Y la verdad es que desde el punto de vista de autentificación digital o electrónica aporta muy poco. Tampoco importa mucho que se haya escaneado la firma holográfica y se haya puesto en JPG el documento. Pero desde el punto de vista de la usabilidad con el ciudadano, es tremendamente potente.

Entonces la pregunta es, ¿dónde está la firma avanzada? Está en las propiedades. Con el lado derecho del mouse, siempre háganlo, pueden entrar a las propiedades y aquí me empieza a hablar con criptografía simétrica.




La información en el certificado digital me está diciendo, que el Sr. Víctor Rebolledo firmó este certificado. Veo los detalles: hay una empresa certificadora, E-sign, que me dice que el Sr. Rebolledo es funcionario del Registro Civil y se responsabiliza legalmente por esto.

Certifica la identidad del firmante en forma avanzada. Este es el aporte de las empresas certificadoras. Se trata de respaldar la identidad de un funcionario, en un documento electrónico cerrado. Puedo ir más allá: me da más información, puedo ver los detalles y me voy a encontrar con el número de serie y con él puedo ir al sitio web de la empresa certificadora, para ver si no está revocado el certificado. Me dice los algoritmos que se usaron. Todo esto es lo que blinda y respalda la identidad del funcionario público que firmó y esto es lo que está regulado en la Ley de firma electrónica. Si tienen esto en mente, de aquí en adelante vamos a poder avanzar con más facilidad.

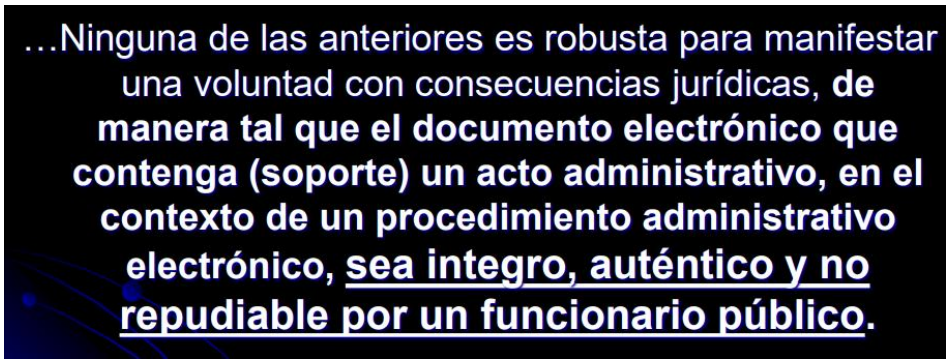

(14:51) Hablemos de autentificación como manifestación de voluntad. Autenticar es verificar identidad del signatario, en dos palabras. Entonces, cualquiera sean los medios electrónicos que se utilicen para esto, lo que hace es que presenta las credenciales del funcionario a un sistema en línea. ¿Puede ser suplantado? Sí, claro, puede ser suplantado. Alguien puede manejar las credenciales del funcionario. Pero a priori hay una apreciación de legalidad, que es lo que establece la Ley de Firma Electrónica. Independiente de cuál sea la tecnología que uno use. Yo puedo usar biometría facial, la huella dactilar, puedo asociar claves y RUT, puedo asociar Clave Única y RUT. Todos los funcionarios, una vez al año cuando se declara el patrimonio se autentican simplemente con RUT y Clave Única. Y eso significa que le dicen al sistema quienes son. Esas presunciones son las que facilitan y

agilizan el flujo documental. Se pueden revertir, por cierto. Uno escucha: “esto es peligroso por la posibilidad de un delito informático”. Todo sistema está abierto a ese tipo de cuestiones, pero en la dinámica del día a día créanme que esto funciona y está instalado. Y esto lo pueden percibir, sobre todo los que sean funcionarios públicos.

Esto es lo importante. Cualquiera sea el mecanismo de autenticación: más robusto o menos robusto, más complejo o menos complejo, con certificados digitales, con doble clave, con mensaje al celular, con sistema de validación, cualquiera sea el sonido, el símbolo o el proceso electrónico, si hay un documento recibido por un receptor, la ley dice que eso va a permitir identificar al menos formalmente al autor de la firma en ese documento. Esta consagración genérica es una norma habilitante que está restringida. ¿Qué pasa si estoy autenticándome pero no firmo un documento electrónico? Algunos dicen que no tendría valor legal, pero al margen de la discusión jurídica, el blindaje normativo ahí está. Como cualquier mecanismo de autentificación en el sector privado. Yo hace muy poco celebré un contrato de compraventa de un seguro para el auto por vía telefónica. El proceso electrónico fue una grabación de voz. Hubo otros sistemas de verificación concurrentes: me preguntaron por mi RUT, me llamaron antes, me mandaron un mensaje corto. Fue robusta la autentificación, pero llegado el minuto de celebrar el contrato, me preguntan derechamente y dije: “Sí, yo quiero el contrato”, y eso quedó registrado, ahí quedó la manifestación de consentimiento sobre un documento electrónico. No puede haber hoy en día, de aquí en adelante, ninguna duda jurídica sobre la validez en Chile de los mecanismos de autenticación. Ahora bien, hay modalidades: hagan el ejercicio de ver cómo se contrata de forma electrónica la apertura de cuenta corriente hoy en día con el Banco de Chile. Van a ver un proceso robusto de autentificación, le van a pedir Clave Única, les van a mandar mensajes, les van a hacer un escaneo de biometría facial, entre otros. Y en algún minuto, vamos a llegar a esto: según ley de Firma Electrónica, conforme a lo establecido por este articulo segundo, al que está mandatando esto, le dicen: ¿usted quiere aceptar el contrato? Me dejan verlo, Ley del Derecho del Consumidor, y al final yo acepto. ¿Dónde queda registrado esto?, en un log transaccional. Y ese Log de registro es un documento electrónico legal en Chile. Ese documento electrónico va a estar autenticado, no firmado con certificados digitales, pero si va a estar autenticado y con pleno valor legal. Esto mismo, en la gestión de los servicios públicos, tiene total blindaje legal, no puede a estas alturas existir ese tipo de cuestionamiento. Créanme que a uno le siguen preguntando: ¿cuál es el alcance jurídico del blindaje?

(18:31) Ya les dije lo del Servicio de Impuestos Internos. Es exactamente lo mismo. En las boletas de honorarios que muchos de ustedes pueden firmar regularmente, no llega a un certificado digital, no hay un cierre específico del documento, pero uno autentica al inicio.

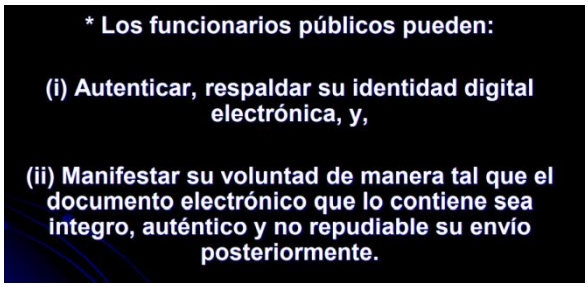
Cuando se entra a una Declaración Anual de Renta, se autenticaron previamente, hay un log que registra la aceptación, ese log es un documento electrónico, ¿verdad? Entonces, si bien es cierto no le doy autonomía a un documento específico que es lo que generan los certificados digitales y la Firma Avanzada, estas autenticaciones con consecuencias jurídicas están totalmente reconocidas en Chile y no admiten cuestionamiento legal.

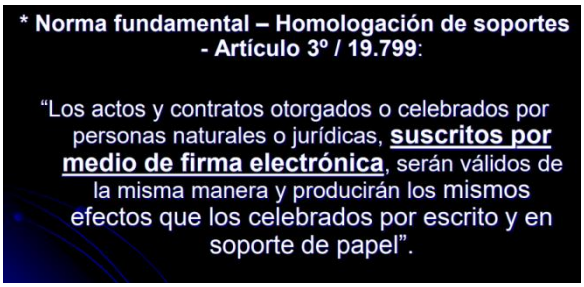



Ahora, el paso siguiente: estos mecanismos de autenticación, no son lo robustos que pueden ser asegurarle autonomía a un documento electrónico, de manera que sea íntegro, auténtico y no repudiable, en este caso por un funcionario público. Por eso la gracia en Chile de los 40 millones de documentos tributarios electrónicos que se emiten mensualmente, que se bastan en sí mismos, que son autónomos, cualquiera que los reciba: la contraparte comercial, un tribunal, el mismo Servicio de Impuestos Internos, tiene total garantía de que esa factura electrónica cerrada, con mecanismos criptográficos, es íntegra, auténtica y no repudiable. Ojo, son presunciones legales las que avalan esto. Alguien podrá decir que le usaron el certificado, que le usaron la clave o que estaba con vacaciones en el Servicio Público y alguien firmó a su nombre. Perfecto, esas son cuestiones de hecho, que se pueden presentar en cualquier sistema de información. Pero esas cuestiones de hecho, puntuales, no deben llevar a cuestionar la validez del sistema y hay mecanismos técnicos para evitar ese tipo de alteraciones mínimas.

(20:14) Les cuento que de los casi 20 años trabajando en esto, no conozco ni una querella por suplantación, no conozco ningún problema de autenticación. Las facturas electrónicas han tenido cero cuestionamientos legales, no conozco ni una sola jurisprudencia, ni siquiera arbitral, respecto a la falta de idoneidad de la autenticación de documentos electrónicos. Entonces, cuando en el mercado de los proveedores uno escucha voces que dicen: “no, la firma avanzada no se masifica, no es segura, etc.” La verdad, esos argumentos son bastante débiles desde el punto de vista de la implementación real y desde el punto de vista del respaldo jurídico.

Hablemos entonces de autenticación criptográfica. Hablemos de estos sistemas más robustos de autenticación, pero que en paralelo al mismo tiempo permiten una manifestación de voluntad. Y hablaremos de aquí en adelante de la PKI, de la infraestructura de llave pública. En resumen, del uso de certificados digitales emitidos por una autoridad certificadora para generar dos claves: públicas y privadas. Y en definitiva, adicionarle materiales criptográficos a un documento, para que pueda ser íntegro, auténtico y no repudiable, eso es en esencia el tema de la PKI.



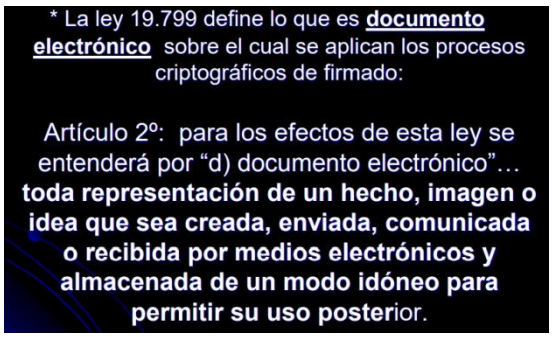



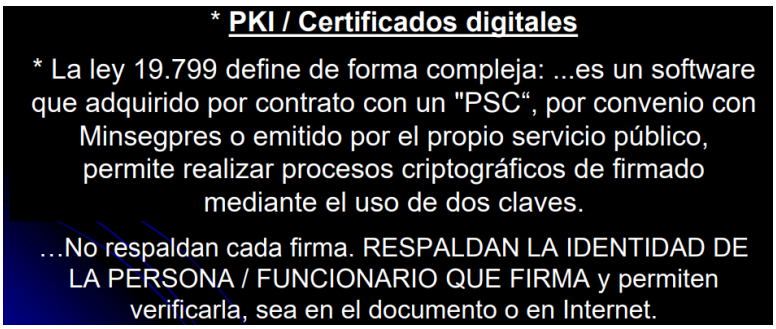

(21:34) Hay un problema inicial, jurídicamente hablando, que hay que despejar, y lo vamos a hacer de inmediato. Con certificados digitales un funcionario público va a poder siempre: "Autenticar, respaldar su identidad digital electrónica". Como les mostré al inicio con el certificado del Registro Civil, lo que hizo la empresa E-sign, por si acaso no soy proveedor comercial, tocó que el certificado está respaldado por esa empresa, es decirle a cualquiera que vea el certificado quien es el funcionario que lo firmó. Eso es la función esencial: proveer confianza, pero al mismo tiempo, va a permitir manifestar voluntad en un documento electrónico y darle a estas propiedades tecnológicas de seguridad con reconocimiento legal al documento que firme. Lo que quiero despejar desde ya, que es un tema que se levanta recurrentemente, relacionado con los posibles cuestionamientos de legalidad y validez.

Algunos dicen: "No sé si esta gestión documental electrónica es lo mismo que el papel del que puedo tener copia y archivar las copias" Téngase presente el artículo 3°. Este artículo es revolucionario, este artículo en el mundo jurídico fue rupturista. Hoy hablamos de tecnologías disruptivas, esto fue tremendamente rupturista y disruptivo. El año 2002 dice lo siguiente: "todo acto administrativo", en este caso o contrato particular celebrado por personas naturales, un funcionario notificando a un ciudadano suscrito por firma electrónica, esa es la barrera de entrada, ese es el requisito para esta consecuencia jurídica. Y dice la norma: "van a ser válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel". Amigos míos, los que no son abogados y están visualizando este artículo, esta es una norma imperativa, manda, no admite interpretación. La doctrina no tiene nada que decir, la jurisprudencia no tiene nada que cuestionar: serán válidos de la misma manera y producirán los mismos efectos que los

celebrados por escritos y soportados de papel. Hay aquí una homologación de soportes derechamente, para el mundo público, para el mundo privado, para las AFP, las Isapres, el mundo comercial, para los documentos comerciales, para la banca, para las operaciones del Servicio Nacional de Aduana, que tiene un flujo de declaración de ingreso de mercancía o de salida importante, todo el sistema jurídico chileno se vio intervenido por este artículo tercero. Esta es otra piedra basal para cualquier construcción en materia de procedimiento administrativos electrónicos, de aquí en adelante. Téngalo siempre presente porque es clave.

(24:05) Estamos firmando documentos electrónicos. La Ley de Firma Electrónica, la Ley de Procedimiento Administrativo, modificada por la Ley 21.180 de Transformación Digital del Estado, habla de medios electrónicos. Esos medios electrónicos son documentos, expedientes y plataformas. La pregunta asociada es: ¿y cómo desarrollamos técnicamente los documentos? Estamos a la espera de las definiciones del reglamento respecto a la implementación, para que haya interoperabilidad y sean estructurados de la misma manera estandarizada los documentos. Pero legalmente, ¿qué valores de entradas hay en este minuto? Ninguna, la definición es genérica, lo importante para el sistema jurídico chileno de cara a la implementación de documentos electrónicos, es que cualquier hecho, cualquier imagen, cualquier idea, una foto, sea creada, enviada, comunicada o recibida por medios electrónicos. No hay restricciones tecnológicas, ni en la ley ni en el reglamento para la implementación. Entonces, definiremos PDF, definiremos XML, porque es mejor estándar por internet. Normativamente, no hay restricciones para la implementación concreta y específica de los documentos electrónicos que van a ser firmados.

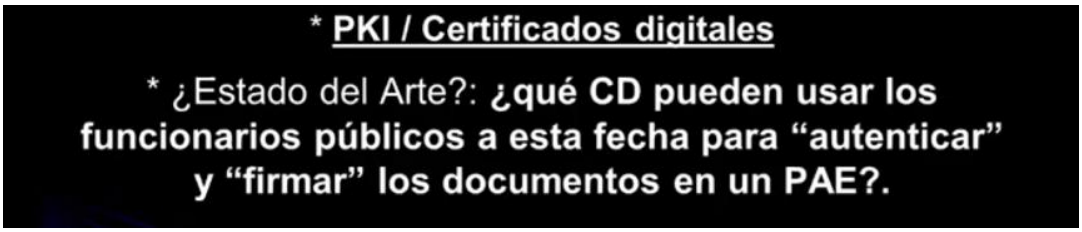


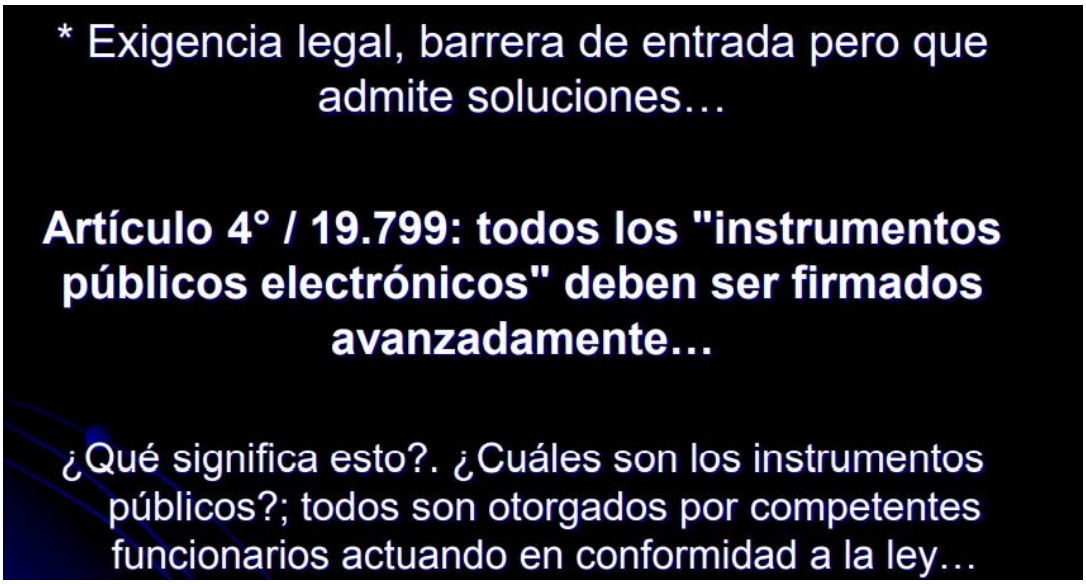




El elemento clave: los certificados digitales. La verdad es que de cara al artículo segundo que define objetivo de la ley, que regula todo esto en el sector público. Para mí son importantes las declaraciones conceptuales, para entender que el elemento clave es tener certificados digitales. El gran problema o la gran definición va a ser dónde los adquiero, ¿Cómo puedo tener esta herramienta de firmado, que genera claves privadas y genera procesos de autenticación criptográficas? Les anticipo: los genera el propio servicio público o las subcontrato con una empresa acreditadora o las adquiero mediante

convenio con MINSEGPRES, o Firma GOB en este minuto. Hay tres opciones claras y con blindaje legal reconocido además, no sólo por la ley sino que por la Contraloría y la Corte Suprema.

Es un certificado digital, la ley tiene una definición algo compleja. En dos palabras, es un software que yo instalo, es un software criptográfico que puedo adquirir por estas tres vías y va a ser el que me permita respaldar la identidad del funcionario, no la firma específica. El certificado lo adquiero un primero de enero de un año y hasta el año siguiente puedo firmar 200.423 documentos que no son conocidos por la entidad certificadora. No sabe la integridad, ni el contenido, ni a qué ciudadano va dirigido. No hay presencialidad, la fe pública descansa en respaldar la identidad en caso de duda, verificando, igual que hicimos al principio, con el certificado de registro no más. Eso también es importante. Y despejamos la firma, los documentos y los certificados.




Estado del Arte, ese es el tema central, y eso es lo que espero que quede despejado con esta breve presentación y después con el coloquio, ¿qué certificados digitales pueden usar después los funcionarios públicos para autenticar y firmar? Copulativamente, ambas propiedades en el marco del procedimiento administrativo electrónico. Ya les mencioné la exigencia legal, la barrera de entrada que está sí o sí establecida, que hay que tener siempre presente. Todos los instrumentos públicos electrónicos deben ser firmados avanzadamente. Todos los documentos públicos deben ser respaldados con certificados

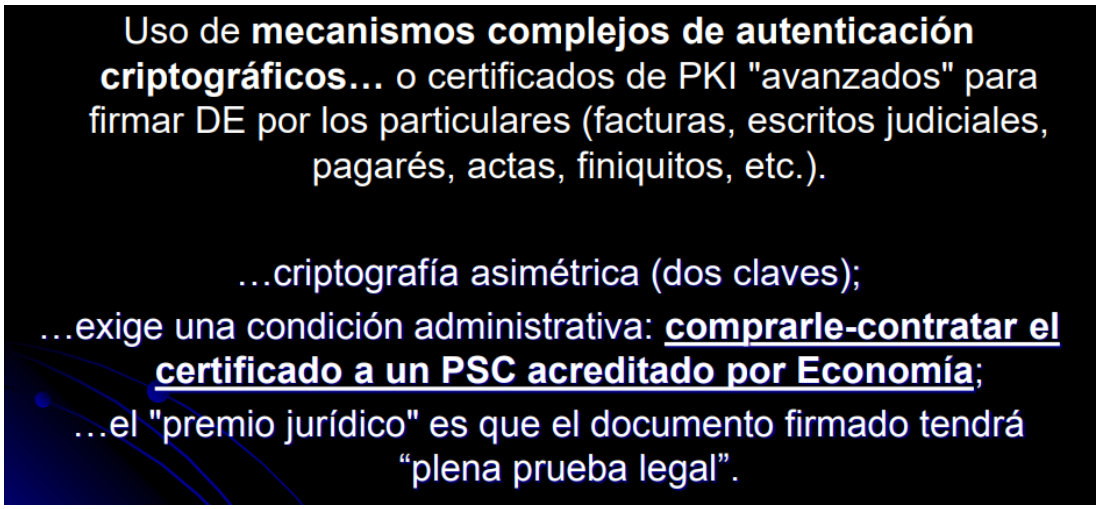
digitales. La pregunta difícil, y esto es para los abogados, es definir: ¿cuáles son los instrumentos públicos de la administración del Estado? Por concepto legal general del derecho chileno, son los otorgados por funcionarios competentes de acuerdo a las formalidades establecidas por la ley, actuando dentro de su competencia. Perfecto, pero el trabajo de detalle de definir, ¿cuáles son aquellos elementos públicos electrónicos? Porque también los servicios públicos gestionan documentos que no tienen esta calidad y en consecuencia no van a necesitar ser firmados con certificados digitales, o avanzadamente, es un trabajo jurídico de largo aliento. Se los digo desde ya, no es difícil hacer estas definiciones, ahora la solución podría ser: por lo general voy a firmar todo avanzadamente para evitar cuestionamientos en materia de auditoría de la Contraloría. Es un criterio también que puede recogerse.

## III. FEA de los particulares.

(28:16) Hay que establecer una diferencia importante entre la Firma Electrónica Avanzada de los particulares y la Firma Electrónica Avanzada del título segundo. Son distintas, obedecen a lógicas jurídicas y tienen blindaje jurídico distinto. Y esto también es importante, porque cuando uno escucha o lee informes en derecho, ve análisis de grandes estudios jurídicos o ve artículos, y dice: “en Chile existen dos tipos de Firma Electrónica, la Simple y la Avanzada” la verdad, es que hay un error fuerte, importante, no menor. **En Chile hay cuatro tipos de Firmas Electrónicas**. Tengo la **simple autenticación**, usada como manifestación de voluntad, ya vimos dos o tres ejemplos. Tengo la posibilidad de **firmar con integridad**, no repudio y autenticación **usando certificados digitales**, pero sin inscribir el certificado de una empresa acreditado por el Ministerio de Economía. Es decir, voy a tener todas las propiedades de la firma electrónica criptográfica robusta, pero no vas a tener el calificativo jurídico de avanzada y lo firmado no tendrá plena prueba, que es un efecto jurídico colateral, por el artículo 5to de la ley. No va a tener ese efecto colateral, pero sí sirve y en el mercado chileno hay empresas en que los mismos proveedores venden los certificados digitales para operar sólo entre los particulares y sin esta consecuencia jurídica de ser avanzada, sin el efecto jurídico de producir plena prueba. Y está la **Firma Electrónica Avanzada** del título segundo de los órganos del Estado, de la administración, del Poder Legislativo y del Poder Judicial, que es distinta, que tiene regulación específica y eso también es tremendamente importante.

Para blindar los desarrollos propietarios de certificados digitales de, por ejemplo, Impuestos Internos, MINSEGPRES, o para blindar un proceso que está creciendo y es tremendamente importante que es aporte, de firma GOB, que está haciendo MINSEGPRES, vía convenio con servicios de Backoffice, para permitir que todos los

servicios públicos puedan acceder a cero costo al uso de esta herramienta de autenticación y firmado. Entonces, cuando a uno le preguntan, y ve sobre todo en el mundo jurídico y los ingenieros que cuestionan esta definición de qué es Firma Electrónica Avanzada en Chile, la primera advertencia: esta definición está en el artículo segundo de la ley y está restringida al sector privado. Esta definición dice que cada vez que tengo un certificado digital, yo controlo la instalación del certificado, controlo el pin de activación, que son los medios exclusivos y podré tener integridad, autenticación y no repudio. La condición administrativa esencial es que le compre software a un prestador acreditado por el Ministerio de Economía. Si no le compro el software a un prestador acreditado del Ministerio de Economía, tendré identidad de autencidad y no repudio, pero no tendré Firma Avanzada y jurídicamente plena prueba. La verdad, que la consecuencia que tenga plena prueba sobre el hecho de haberse otorgado, las partes que lo otorgaron, el contenido del documento, etc., tampoco ha sido materia de ningún cuestionamiento judicial, del año 2003 a la fecha. Es un efecto de la robustez jurídica, en este caso de cara al flujo documental en el sector privado de documentos electrónicos, y en el sector público ha tenido cero cuestionamientos también.




(31:19) De qué estamos hablando cuando se habla de Firma Avanzada: criptografía simétrica, dos claves, autenticación robusta, adquisición del certificado de un prestador acreditado por Economía y este valor legal de la plena prueba. Esto en el sector privado.

Cuando vamos al sector público título segundo las definiciones son distintas, las exigencias son distintas, pero las consecuencias jurídicas, los efectos, son exactamente los mismos, plenos y de valor legal. ¿Qué pasa con el título segundo de la ley de Firma Electrónica? está blindado, ha sido implementado, desarrollado, validado por la Contraloría General de la República y por la Corte Suprema, para respaldar todos los nuevos procedimientos electrónicos del Estado.

# IV. FEA del Título II de la ley 19.799.

¿Qué es este título segundo? Primero, un reconocimiento y una explicación.

Santiago de Chile, Jueves 26 de Agosto de 1999

## La Firma Digital Remecerá el Estado

**Cuando los presidentes de Chile y Argentina firmaron un acuerdo de manera digital el viernes le dieron el puntapié inicial a la modernización armónica de ambos países.**

Nunca dos mandatarios de América Latina habían firmado un acuerdo de manera digital. Frei y Menem tienen este récord. Pretenden asegurar que las tecnologías que se aplicarán en Chile y Argentina sean compatibles.

En el futuro, los sectores públicos de ambos países se podrán comunicar electrónicamente con firmas digitales que garanticen que los remitentes son quienes dicen ser.

Argentina trabaja hace dos años en la firma digital, informó Juan Franchino, el subsecretario de Gestión del Sector Público que venía en la delegación transandina. La semana pasada, Menem envió al Parlamento un proyecto de ley de firma digital para el sector privado.

Cuando se trabajaba en el proyecto de Ley de Firma Electrónica y uno iba a las reuniones y hacía observaciones, de a poco, estamos hablando del año 2000, 2001, la Ley se aprobó el 2003, el nivel de usabilidad de certificado digital era mínimo, los niveles de autorización eran tremendos. En ese entonces había vigente, del año 99, el Decreto Supremo 81, sobre el uso de Firma Electrónica en los órganos del Estado. Se pescó ese decreto 81, sus disposiciones y se incrustó en la Ley de Firma Electrónica. Es decir, ese título segundo no obedece a la lógica y a las definiciones generales de la ley, por eso los errores conceptuales. Igual mi reconocimiento a don Claudio Orrego, expresamente porque tuvo una asertividad, una impulsividad, una creatividad y una capacidad en ese entonces de partir con las primeras regulaciones sobre el uso de firma electrónica en el Estado. Y también su lugarteniente, mi reconocimiento a mi amigo don Enrique Rajevic, profesor de Derecho Administrativo, porque fueron capaces el año 99 de desarrollar este tipo de marcos normativos. Entonces tenemos 21 años de regulación sobre el tema. Hoy el 2020,

creo que nadie visualizaba lo que esto iba a crecer, pero bueno, se desarrolló, están las normas y eso es lo que vamos a revisar.

| ESTRUCTURA DE LA PKI | PKI SECTOR PRIVADO | PKI SECTOR PÚBLICO |
|---|---|---|
| ORGANISMO ACREDITADOR | SUBSECRETARIA DE ECONOMÍA | LA LEY DEL TITULO II / 19.799 |
| AUTORIDAD DE REGISTRO / RA | PSC / Notarios - OSRC | MINISTRO DE FE |
| AUTORIDAD CERTIFICADORA / CA | PSC / ACREDITADO | - PROPIO SERVICIO PÚBLICO (SII)<br>- PSC ACREDITADO<br>- MINSEGPRES |

(33:55) Una explicación conceptual del esquema estructural, que es tremendamente importante. En la tercera columna, está el título segundo. La primera columna, a la izquierda, es la explicación técnica de toda estructura de certificados digitales, PKI, infraestructura de llave pública, en inglés. En todo sistema, que lo pueden representar también piramidalmente, hay un organismo acreditador, que técnicamente es un organismo que también emite certificados digitales. Sus claves públicas se incorporan a los certificados digitales del segundo nivel, que son las empresas certificadoras, que hacen siempre dos funciones copulativas. Toda empresa de certificados tiene que cumplir dos roles: la autoridad de registro, verificación de antecedentes y verificación de que ellos sean. En segundo lugar, como autoridad certificadora emiten el software certificador, verifica la identidad y emite el software o certificado digital que respalda la identidad y permite generar las claves públicas y privadas, para hacer el cifrado en flujo (stream) de cierre criptográfico, y dar la integridad, autenticación y no repudio a los documentos que se firmen.

La columna del medio corresponde al sector privado. ¿Quién es el organismo acreditador en Chile? La Sub-secretaría de Economía, sólo para el sector privado. Este es otro tema también que recurrentemente aparece: ¿será la Subsecretaría de Economía competente para acreditar a MINSEGPRES o a los servicios públicos? De ninguna manera. Porque eso es derecho público. Si alguien hubiera querido que el título segundo pasara por la gestión de la Sub-secretaría de Economía, tendría que haberse dicho expresamente en la ley. El

derecho público no se interpreta, si no está regulado no existe derecho público. Pero bueno, en el sector privado, acredita la Sub-secretaría de Economía. Las empresas certificadoras acreditadas, son las que emiten los softwares de respaldo, para los operacionales firmados. Y las autoridades de registro pueden ser, por prestador de servicio de certificación o notarios, u oficiales del Registro Civil, previo convenio con los prestadores de servicio de certificación. Eso es la PKI, la Firma Electrónica Avanzada en el sector privado.

Al sector público, esto es importante, el primer nivel, ¿quién acredita? El artículo 9° de la ley de firma electrónica acreditó, definió la Firma Electrónica Avanzada, y empoderó, tienen la autoridad de registro, en el título segundo, los ministros de fe de cada servicio. Son imprescindibles. Si un Ministro de fe no habilita a un funcionario previamente por resoluciones expresas para firmar, está actuando en forma ilegal. Jurídicamente el ministro de fe en cada servicio público tiene connotaciones distintas, si es una municipalidad es el Secretario municipal, en algunos servicios es el Director del Servicio, en otros el ministro de fe está determinado por resolución, etc.

Y el tercer nivel de esta estructura de uso de certificados digitales: ¿Quiénes pueden emitir estos certificados, quiénes pueden habilitar estas herramientas de firmado? Primero, el propio servicio público, certificando la identidad del funcionario. Vamos a ver que el artículo 9° habla de certificar la firma del funcionario. Espero que haya quedado despejado que lo que queda respaldado es la identidad del funcionario y no cada firma concreta, no ve cada documento firmado el que respalda la identidad. El propio servicio público. Un caso concreto, desde el 2007 a la fecha, es un proyecto robusto, sólido y que funciona, todos los funcionarios de Impuestos Internos usan sus certificados digitales. Caso segundo: MINSEGPRES. No conozco otros. Alguien me dijo que la Armada está desarrollando su propio sistema de certificación. Bien, si tiene los elementos tecnológicos, porque es complejo tener un laboratorio de certificados digitales, es un tema criptográfico, no es tan simple. Si el propio servicio público no puede desarrollar el software, lo puede emitir un servicio acreditado previamente por el Ministerio de Economía, lo dice expresamente el inciso 4to del artículo 9°.

Y lo más importante, lo más revolucionario es la tercera opción, hoy en día. Es lo que hace MINSEGPRES, validado por la Corte Suprema, respaldado por los dictámenes de la Contraloría, que no asume formalmente un rol de certificador, sino hace una operación de Backoffice. Ojo, la Ley de Bases establece la colaboración obligatoria en materia de recursos entre servicios públicos. El MINSEGPRES le dice al servicio público: “mira, te presto mi salida, firma acá, auténtica los documentos acá gratuitamente”. Disponibiliza esta herramienta para que tú como servicio público, y tú Ministro de fe, generen acá sus

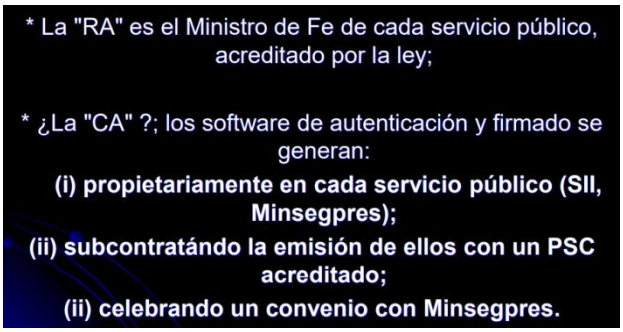
herramientas de firmado. El sistema de Firma Digital ha crecido y funciona, tiene videos explicativos en YouTube, hacen cursos de capacitación. Yo creo que de aquí en adelante al ser este sistema implementado por Firma de Gobierno se puede producir una real masificación. ¿A quién le sirve esto? A los servicios públicos de menor envergadura, de menor presupuesto y de menor cantidad de funcionarios. Les facilitó la generación de las herramientas de firmado, y lo importante: es plenamente legal, con este título segundo de la ley de Firma Electrónica. Si estas estructuras conceptuales del mercado existente hasta la fecha se entendió, no vamos a tener ningún problema con avanzar con la lectura de los artículos.

Este artículo es clave, en dos palabras, vamos rápidamente: Art. N° 9 "La certificación de las firmas electrónicas avanzadas… (No es cualquier firma, y produce plena prueba según el artículo 5° de la ley)…de las autoridades o funcionarios de los órganos del Estado (Solamente los funcionarios de los órganos del Estado. Pregunta: ¿puede el Estado certificar a un ciudadano? No puede. ¿Puede un servicio público respaldar a los contribuyentes? No puede, sólo respalda la identidad de sus propios funcionarios)…se realizará por los respectivos ministros de fe". (Clarísimo: se realizará. Aquí no hay "la doctrina dice", que les gusta mucho a los abogados. Aquí no dice nada de doctrina, simplemente reconocer una norma imperativa. "La jurisprudencia ha dicho". No hay jurisprudencia. Desde el año 2003 a la fecha no hay ni siquiera jurisprudencia a nivel de arbitraje, pero sí hay dos dictámenes de la Contraloría General de la República que validan y blindan esto, y que para mí es suficiente asidero, más un fallo de la Corte Suprema que se los voy a mencionar en algunos minutos.

¿Qué dice esta ley en el inciso segundo? Esta certificación (no es de la Firma Avanzada generada o aplicada a un documento en concreto, sino de la identidad del asignatario que firmó o del funcionario que firma), este software firmado, tiene que tener menciones y fechas y hora de la emisión. Las emisiones son los campos o documento electrónico, amigos míos. Uno lo visualiza en pantalla en el PDF, pero estructuralmente tiene campos de información. Los certificados digitales deben tener el RUT del funcionario, el mail del funcionario, el cargo que ocupa en el servicio público y la vigencia de esa herramienta de firmado, con definiciones técnicas que están sub-sumidas en esta explicación.

Pero esto es lo importante: el inciso tercero en este artículo 9°. Si lo tienen retenido de aquí en adelante, yo me voy tranquilo con este resumen apretado del "Estado del Arte", porque esto es la ley vigente, acuérdense "Estado del Arte", ley vigente. ¿Qué dice este inciso tercero? Los efectos probatorios de la certificación practicada por el Ministro de fe competente…(Es decir, las consecuencias jurídicas del hecho de haberse firmado un acto administrativo usando certificados digitales, previa habilitación del Ministro de fe del

servicio público)…son equivalentes a los de la certificación realizada por un prestador acreditado de servicios de certificación. (Son equivalentes jurídicamente, son equivalentes técnicamente, pero son distintos)


No hay un enclave cerrado ni una obligatoriedad, por la definición de Firma Avanzada, de sólo usar certificados adquiridos a empresas particulares. Lástima para el negocio de las empresas particulares. Esta equivalencia valida el uso de certificados digitales dentro de la administración del Estado, al margen que son lo mismo, son equivalentes jurídicamente y técnicamente, pudo haberse precisado cuando yo adquiero herramientas de firmado con empresas particulares.

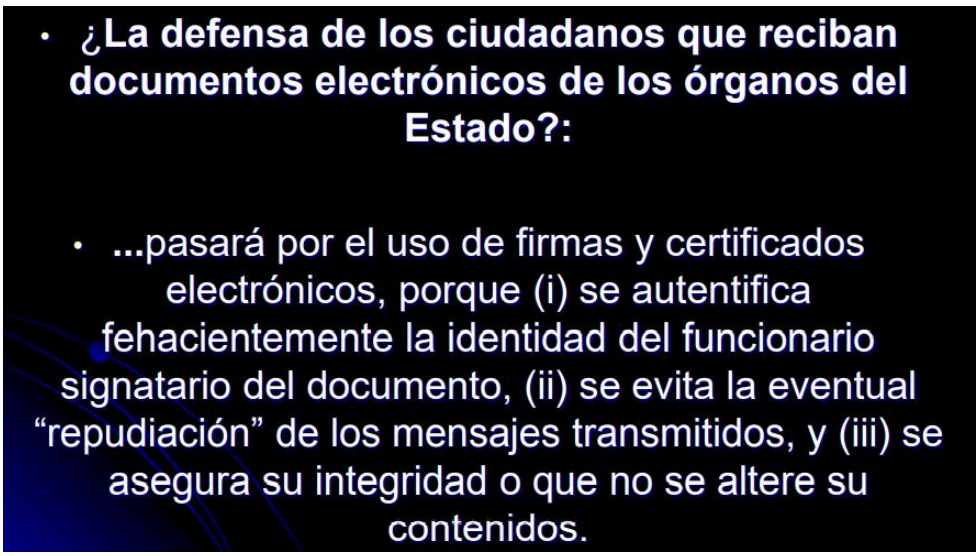
Si esto no estuviera claro a estas alturas, el inciso cuarto de este artículo 9° lo termina de cerrar, cuando dice: "Sin perjuicio de lo dispuesto en el inciso primero… (o sea, sin prejuicio que un propio Ministro de fe defina quienes van a ser los funcionarios habilitados para firmar, sea por resolución o reglamento. El artículo 10° exige un reglamento que los servicios públicos hasta la fecha no han dictado, salvo Impuestos Internos y con oficio circular 13 que pueden ver en su página) Dice: Sin perjuicio de esta certificación que realiza el ministro de fe se pueden contratar, léase subcontratar los servicios, certificación con empresas acreditadas por Economía, ¿cuándo? Cuando sea más conveniente técnica o económicamente. Y es verdad, porque una municipalidad del sur de Chile, de una comuna pequeña, no tiene el andamiaje, no tiene presupuesto para implementar esto. Hoy en día tiene dos opciones: o subcontrata la adquisición del certificado de autenticación robusto de PKI de una empresa o, usa la opción que está penetrando, que se está implementando y que funciona técnicamente y tiene blindaje jurídico, lo adquiere de manera gratuita, previo convenio con MINSEGPRES.

(43:06) Ayer hacíamos un curso de estos temas, un excelente curso en la Universidad Alberto Hurtado, y muchos de los asistentes ya están utilizando la herramienta de firmado provista por Firma gob.cl. O sea, espero que con estas precisiones quedan absolutamente de lado los posibles cuestionamientos legales frente a la pregunta inicial: ¿cuál es el "Estado De Arte" regulatorio de esto? Aquí está. Este es, no hay otro: la certificación de la Firma Electrónica Avanzada la hace el Ministro de fe. Ya aclaré los certificados, la

identidad del firmante. Y esta certificación tiene dos funciones: lo presencial, lo registral, lo administrativo, ver que el funcionario sea funcionario, que no lo hayan dado de baja, no haya renunciado al servicio. Y la segunda función: la emisión del certificado digital que va a respaldar la identidad cuando firme en concreto un documento que contenga un acto administrativo dentro de un procedimiento administrativo que son los regulados por la ley 19.880 de manera general y supletoria o por las leyes especiales.

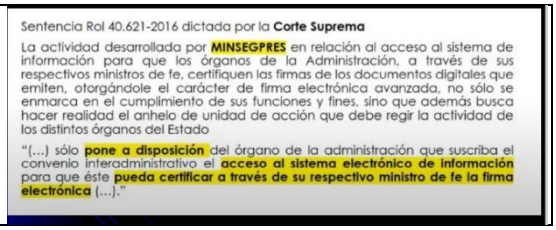
(44:13) Entonces, claridad absoluta tengo del Ministro de fe que valida a los funcionarios, perfecto. Y el software, ¿dónde lo adquiero? O lo emite cada servicio público, Impuestos Internos desde el año 2007, MINSEGPRES para sus propios funcionarios, o subcontrato la emisión con un prestador acreditado. Perfecto. Los prestadores acreditados están publicados y respaldados por la Subsecretaría de economía. O la opción más potente, desde el punto de vista de la masificación: un convenio con MINSEGPRES que me permite entrar a usar un servidor HSM.

Hace un tiempo, antes del Cloud computing, de la externalización a la nube, se hablaba mucho de los contratos de hosting y housing. en dos palabras, el hosting me permitía autorizar ciertas aplicaciones de un servidor provistas por el propietario de este servidor, y el housing significaba que yo sub arrendaba el espacio y entraba con toda mi tecnología y gestionaba internamente mis sistemas, mis documentos, mis bases de datos en este servidor. Lo que hace MINSEGRES se acerca mucho al housing, porque permite la autogestión de cada servicio. Entonces, no es MINSEGPRES el que esté realizando, sino que dentro del título segundo, disponibiliza, previo convenio de colaboración según la Ley general de bases, de las herramientas de firmado.




¿Qué es lo importante jurídicamente para el ciudadano o el contribuyente en Impuestos Internos, de la Tesorería, para el ciudadano en general? Si yo tengo un documento que me

llega con la notificación administrativa de un proceso, sea que me llega directamente a mi correo, sea que esté disponibilizado en una casilla electrónica. Estamos a la espera de ver cómo va a ser la notificación legal general reglamentada en el marco de la ley 21.180, como sea su proceso tecnológico. Si recibí un documento firmado con certificados digitales avanzados, en el contexto del título segundo. Esa es la vigencia actual del sistema. El ciudadano va a saber que el funcionario que firmó era quien dice ser, el funcionario que firmó no va a poder repudiar el envío del documento electrónico, y ese documento le llegó íntegro, auténtico, desde el punto de vista de su contenido. Si se altera la integridad de la notificación al ciudadano le llega un chorizo ininteligible de códigos binarios que no dicen nada. Si llega estructurado y se lee el contenido, es porque la integridad se mantuvo. Si tengo dudas, acuérdense de la diapositiva del inicio cuando verificamos el certificado del Registro Civil. Esos son los procesos de validación. Me habla el propio documento. O incluso más, me puedo conectar al sitio web de MINSEGPRES o de la entidad certificadora y ver si la firma utilizada está vigente en el llamado CRL, un término técnico de la lista de claves públicas de los certificados revocados. Ese blindaje es para las dos partes de la punta de un procedimiento administrativo electrónico: cobertura total para los ciudadanos y habilitación completa, técnica y legal, para los funcionarios públicos que respalden cualquier documento.

| | |
|---|---|
| * La **Contraloría general de la República** ha dictaminado expresamente el año 2004 (Dictamen 4941) y el año 2010 (Dictamen 75.481) y aplicando la ley 19.799 en su Título II. |  |

Ahí tienen los dictámenes, pueden revisarlos después, de la Contraloría general de la República el 4.941 de 2004 y el 75.481 de 2010 que hablan de la Firma Electrónica Avanzada del título 2° como un espacio autónomo de la propia gestión de los Servicios Públicos y reconocen todo lo que les he dicho.

(47:38) Un fallo de la Corte Suprema, Rol 40.621 del año 2016, a propósito de la implementación del sistema MINSEGPRES, dice expresamente qué es lo que hace al poner Firma GOB a disposición del órgano de la administración del Estado. Sería complejo que MINSEGPRES quiera firmar y respaldar la identidad del Poder Judicial, yo creo que no puede; o del Poder Legislativo, tampoco puede, porque estamos hablando que MINSEGPRES tiene competencias legales de Derecho Público para respaldar la identidad de los integrantes de la administración del Estado, el Poder Ejecutivo. Dijo la Corte Suprema en este fallo, que fue a propósito de la interposición de un amparo económico invocado por el Decreto Ley 211 de libre competencia. Bueno, MINSEGPRES no cobra, por

eso no impacta en el mercado desde el punto de vista económico. Dijo la Corte Suprema: "Sólo pone a disposición de cada órgano o servicio público, mediante un convenio administrativo interno". Si a alguno le interesa, el convenio se lo voy a dejar a disposición de los organizadores del coloquio, para que después se los haga llegar. Me permite el acceso a un sistema electrónico para que pueda certificar con su propio Ministro de fe, autogestionando el respaldo de la identidad digital de cada servicio público. Es un backoffice, es una externalización, es una operación de housing y tiene total valor legal según la Ley en su título II, según la Contraloría y según la Corte Suprema.



(49:10) Ahí está la plataforma de MINGSEGPRES. Ojo, no es que yo venga a hacer apología, es que esto me parece muy rupturista y está operando, funciona. Los funcionarios públicos de Chile, de cara a los procedimientos electrónicos especiales que hay en curso, están utilizando estos certificados digitales. En YouTube hay videos explicativos, está la información completa.

Yo simplemente quiero remitirme, a propósito de la llamada solución SEGPRES, para poner el énfasis en el alcance: hay una autoridad certificadora disponible para todas las instituciones que hagan uso de estos sistemas, herramientas criptográficas de autentificación robusta y de firmado asociado, cumple los dos roles. Autogestionen en lo administrativo con sus Ministros de fe, la emisión de los certificados. Y el resultado: que todo lo que se firme con esos certificados digitales, va a tener la plena prueba de la Firma Electrónica Avanzada, regulada por la ley en el título segundo, que no la cubre estos alcances, la definición del artículo segundo de Firma Electrónica que está pensada en el límite y solamente se refiere al sector privado. Entonces, desde el punto de vista de la masificación, los desarrollos propietarios en materia de autenticación robusta con certificados digitales y firmados, de Impuestos Internos, de MINSEGPRES entiendo que también de la Armada, pero puede que me equivoque. En fin, el servicio público que puede hacerlo. Los que no pueden hacerlo tienen acá una herramienta habilitante con pleno valor legal a esta fecha.

Amigos míos, esto es el Estado del Arte, en mi opinión, esto es el blindaje esencial, básico, con el cual podemos operar, esto es lo vigente, estos son los alcances de la autenticación.

Y en materia de firmado espero haber sido claro para que podamos conversar libremente sobre esto. Muchas gracias y quedo a disposición de las consultas y la conversación.

-Roxana: (51:29) Muchas gracias Renato, excelente la presentación, las precisiones que hiciste son tremendamente útiles porque a veces es difícil distinguir algunos alcances que hiciste. A mí en particular me pega fuerte que no es lo mismo la Firma Electrónica del Estado frente a la de los particulares. Y quisiera abrir las preguntas, porque hay muchas y son bastante contundentes. Benjamín Blanco, tiene una precisión respecto del artículo 3° de la Ley 19.799: da la sensación que no hace diferencias entre la Firma Avanzada y la Simple.

-Renato: Es correcto, no hay definición. Cualquier mecanismo de autenticación puede llegar a tener ese alcance. En la definición subsume, tanto la identificación con efectos jurídicos de manifestación de voluntad como el uso de certificados digitales.

-Roxana: Claudio Delgado pregunta: las legislaciones define Firma Avanzada ¿por qué la Entidad Acreditadora define Firma biométrica, móvil y también sello del tiempo si la Ley no lo define? ¿Los conceptos FEA Bio y Sello de Tiempo tienen sustento legal?

-Renato: Sí, por supuesto. Uno: la definición de Firma Electrónica Avanzada que existe en el artículo 2° que expuse en la diapositiva, que la conduce, la limita o la restringe a los prestadores acreditados por Economía, sólo opera en el sector privado. No es proyectable al sector público y los órganos del Estado. En los órganos del Estado puede haber Firma Avanzada, usando un certificado digital. La Firma que existe en la ley es válida para el sector privado plenamente. Segundo, si leen el artículo 5° de la ley se habla del sellado de tiempo: “Sin embargo, no harán fe respecto de su fecha, a menos que ésta conste a través de un fechado electrónico otorgado por un prestador acreditado”. Dice que de manera voluntaria, de manera facultativa, pueden tener, para hacerse respecto a la fecha un mecanismo de fechado electrónico otorgado por un prestador acreditado o servicio de certificación. Ahí está el margen del sello de tiempo. ¿Qué pasó? Estas son las definiciones legales que son bien limitadas y restringidas. Si me voy al reglamento no hay mayor precisión de esto. Entonces, las bajadas han sido por la vía de la interpretación y por la vía de algunas resoluciones exentas que ha dictado la Subsecretaría de Economía.

Por ejemplo, a propósito de la biometría, que es la pregunta específica, cuando el artículo segundo habla de cualquier mecanismo que permite identificar formalmente al autor, de la subscripción de un documento, la huella dactilar digitalizada, recogida y después transferida por un tercero a un documento, una compraventa electrónica de seguros, o cualquier otro documento que aparece representada gráficamente, es un mecanismo

biométrico que al menos, formalmente, permite identificar al autor, si la definición del marco conceptual es general.

¿Qué ha pasado? Que la Subsecretaría de Economía, dictando resoluciones, de hecho tres, habla de biometría facial, de biometría de huella dactilar, etc. Pero tengo un problema serio con eso y lo voy a dejar planteado, porque ya lo he dicho en exposiciones en el Senado. Están los documentos arriba de la mesa, están las presentaciones, si buscan el boletín 8.466, que contiene el Proyecto de Ley que se está debatiendo para modificar todo esto. A mí me sorprendió y es un tema que debe precisarse, validar y revisarse, que estás guías de acreditación biométrica dactilar, facial o de uso de sellos de tiempo, se dicten por resoluciones exentas y no por un decreto supremo específico. Ahí hay un punto jurídico importante. La Subsecretaría de Economía no tiene facultades normativas de dictar resoluciones. No obstante a eso las dictó y en base a esos fundamentos se implementaron los desarrollos biométricos. Sí tiene fundamento legal en la definición amplia de Firma Electrónica no Avanzada o sin certificados digitales, es efectivo, porque son mecanismos que permiten al menos autenticar formalmente al autor, entonces en esa norma genérica está validada la biometría.

El sello de tiempo tiene referencias expresas en el artículo 5°, pero como mecanismo alternativo. Otra complicación que tengo, son inquietudes académicas y las quiero plantear, es: el Proyecto de Ley quiere obligar al uso de sellado de tiempo. Entonces el mito que existe, que se dice que contrato adicionalmente, no sólo el uso de un certificado, si no que si compro un servicio de sellado de tiempo, presenta una tecnología distinta y va a haber mayor robustez en los documentos firmados y la gente va a tener mayor confianza, y nadie va a cuestionar la fecha y la hora de los documentos solamente firmados y no sellado de tiempo. El sellado de tiempo es un proceso adicional. Quiero firmar una factura, tengo mi certificado digital, genero el stream de cierre, tengo autenticación de identificación y no repudio, listo. Y antes de mandárselo a mi contraparte comercial, lo subo al sitio web de la empresa certificadora, le hace unos nuevos procesos tecnológicos, nadie ha dicho cuánto va a costar ese proceso tecnológico. Es como la maleta de los aeropuertos, pongo la huincha adicional. Hoy en día se la pone el que quiere usar sello de tiempo. La ley quiere obligar a que se use y eso yo creo que va a ser una regla de entrada porque va a encarecer los puntos de gestión, y no lo comparto.

(57:31) Pero respondiendo derechamente: en el marco conceptual general de Firma Electrónica no en base a certificados, no de forma avanzada, no criptográfica, no robusta, admite la implementación de cualquier mecanismo tecnológico de cara a la biometría en Chile. Y el sellado de tiempo es un proceso tecnológico adicional, le da mayor certeza

respecto a la fecha y la hora  a la emisión del documento, y también tiene reconocimiento expreso, pero no es obligatorio en el artículo 5° de la ley.

-Roxana: Nos preguntan Claudio si una PSCA, puede “descansar” sobre los Ministros de fe en organismos del Estado para la emisión de Firma Electrónica para un funcionario público. ¿Puedes ampliar la pregunta?

-Claudio Delgado: (58:34) He estudiado mucho tiempo el tema de Firma Electrónica y también, como trabajamos con Andrés Arellano en SEGPRES, en montar el tema de Firma Electrónica en el Estado. La primera pregunta de Firma Avanzada Biométrica y todo eso que la industria en el mundo privado ha generado discusión últimamente en notarías y cosas así, de la aceptación de la biometría como mecanismo de autenticación robusto y de certificación por los prestadores de servicios de acreditación. Entonces hay muchos “clientes” del mundo privado que dicen que básicamente es una Firma electrónica biométrica, la certificación de firma electrónica biométrica o de móvil, la verdad es que la única que existe es la Firma Electrónica Avanzada, entonces esa era la primera pregunta. Y con respecto al sello de tiempo, también va a haber una penetración en la industria que va a encarecer los costos con el tema de sello de tiempo. Pero ese es un tema legal, yo soy ingeniero, entonces la verdad es que desconozco si una escritura o un documento tienen que ir con fecha y hora. Esa es la primera pregunta que estaba haciendo y gracias por responderla. Me quedó muy claro tu punto de vista.

Y con respecto a la segunda pregunta: siempre se ha discutido mucho en el mundo público de esta mezcla entre el prestador de servicio de acreditación que está avalado por el Ministerio de Economía y también la emisión de los certificados por los Ministros de fe. En realidad, la validación de los certificados por los Ministros de fe de cada uno de los órganos del Estado. Entonces también hay una mezcla, hay como un punto medio y esa es la segunda pregunta: ¿si un prestador de servicio de acreditación, puede utilizar la certificación de un Ministro de fe de un órgano del Estado, para emitirle a un funcionario público? Yo lo que entiendo es que la ley dice que un prestador de servicios de acreditación puede utilizar la certificación del Registro Civil, su propia certificación o la de un Notario para la emisión de certificados digitales, pero también estaba en discusión ese otro punto. Gracias.

-Renato: Súper interesante la pregunta. Partamos por lo segundo. Cuando la ley vigente dice en el artículo 12 letra e), respecto a la verificación de identidad, previa a la emisión de certificados, la autorización de registro la puede hacer el propio prestador de servicios de certificación, la misma autoridad certificadora, porque este prestador de servicios de certificación, está copiado de la ley española y son las CA, las autoridades certificadoras. Cuando dice en la verificación de identidad previa, función de registro, la puede hacer la

propia certificadora o la puede delegar a un convenio vía notario u oficial de Registro Civil, eso aplica solamente para el sector privado.

Cuando me voy al sector público, en este título II que insistí tanto, la ley me dice otra cosa. La ley me dice que la función de registro siempre la va a hacer el Ministro de fe y la habilitación para tener el software de firma, lo hace el Ministro de fe de cada servicio público. Eso es una piedra de tope. Situación distinta de la verificación de la identidad. Pero me agrega la misma ley en el artículo 9° inciso 4°, léelo, revísalo, búscalo y márcalo. Ese inciso 4° dice: en el sector público para los órganos del Estado, si el servicio público no es capaz de generar el certificado, no es capaz de tener un laboratorio de PKI, porque es muy costoso, porque es complejo además, puede sub-contratar con la entidad certificadora acreditada por Economía, solamente la emisión del certificado. Entonces acá, no vienen los notarios, acá el respaldo de identidad no lo hace el PCC, acá no hay oficiales del Registro Civil, fue el Ministro de fe del servicio el que le dice al prestador de certificación, yo te hice la pega previa de RA, ahora te pago y generas un certificado para estos funcionarios, porque yo como Ministro de fe los habilito para representar el servicio en el marco de los procedimientos administrativos electrónicos solamente.

(01:02:48) Y respecto a lo primero, agradezco la precisión. Efectivamente el mercado ha distorsionado los conceptos. no voy a dar el nombre de la empresa, pero hay conceptos que no existen. Se habla de una "Firma Biométrica Avanzada". Conceptualmente y legalmente no existe eso, sólo existe la Firma respaldada por el certificado digital. Lo que ha hecho este emprendimiento, de esta empresa certificadora en el mercado, en vez de verificar la identidad presencialmente, llamándolo por teléfono, o de que vaya a la oficina directamente y que firme el contrato y que pague por internet, para apurar los procesos ha dicho: "oye, la parte verificación de identidad hazlo con tu huella dactilar. O la parte de verificación por carnet de identidad, yo te escaneo gráficamente la imagen". Pero ese es un invento comercial de una de las empresas certificadora. Lo que sí está regulado es esta norma específica de la Subsecretaría de Economía, por una Resolución exenta que debiera ser Decreto Supremo para tener blindaje jurídico. Pero bueno, está la Resolución exenta en este minuto, ¿qué es lo que ha regulado? Solamente el uso de biometría dactilar, no hay una regulación ni legal ni reglamentaria, ni a nivel de resoluciones administrativas de Economía del uso de biometría facial. Y por eso se cuestiona en el mercado el uso de "biometría facial avanzada". Es un concepto comercial. Y también, esto es transparencia, hay una presentación expresa en contra de esta empresa para objetar el uso de biometría facial "como respaldo de la autenticación de documentos electrónicos". Esto surgió a propósito de la gestión registral, que también quiero despejarlo brevemente, porque el tema ha estado muy bullado en el mercado. El punto no está en oponerse a las

implementaciones tecnológicas, con usar estos mecanismos, el punto está en que válidamente quienes tienen que respaldar la idoneidad lo hagan normativamente.

En el caso del mundo registral, requiere modificar un auto acordado de la Corte Suprema que está dictado el 2006 y estableció restricciones de operación. Si modifican esa reglamentación que se llama auto acordado, podrán volar otros mecanismos de autenticación, por ejemplo, la biometría facial, pero eso no ha pasado. De hecho el mercado, de hecho dos empresas, pero una en especial, han pasado por sobre la regulación específica reglamentaría al implementar estos sistemas. Por eso se dice que no tiene blindaje legal y es correcto, pero no sé Claudio si con eso se termine de precisar los elementos consultados.

-Claudio Delgado: Sí, muchas gracias Renato.

-Roxana: Yo puedo aportar un ejemplo, que tal vez ayude a despejar. Cuando empezamos a utilizar Firma Digital Avanzada hace muchos años, se hacía con los procedimientos de que la persona iba al notario y hacía todo su papeleo. Cuando estas personas se iban, cuando queríamos caducar esas firmas, no teníamos derecho a caducarlas porque eran consideradas personales y, por lo tanto, desde ahí, de caer en esa cuenta empezamos a usar el proceso a través de un Ministro de fe, pues ahí manteníamos el control, y podemos caducar sin inconvenientes. Y eso a veces no es tan claro para la mayoría. A nosotros nos pasó.

-Renato: (01:06:20) Lo que tú has dicho es la doctrina y la postura de la interpretación correcta. Sólo te voy a precisar conceptos. Cuando yo quiero dejar sin efecto un certificado, por ejemplo, y el funcionario dejó de trabajar en servicio, el concepto técnico es que yo revoco el certificado. La caducidad está dada por el vencimiento. Entonces precisamente, el título II, dice eso. El Ministro de fe, así como me habilitó, me deshabilita. Independientemente de que técnicamente al certificado le queden 6 meses de vigencia, se revoca. Quien lo remitió, lo revoca y lo deja sin efecto por instrucción del Ministro de fe. Eso es propiamente el título II de la Ley de firma. Excelente. Es un buen ejemplo.

-Roxana: Gracias. Y de ahí descubrimos que era la única manera de mantener el control de las firmas habilitantes. Tengo más preguntas, nuevamente de Benjamín: El acto por el que el Ministro de fe habilita la firma de un funcionario, no debe declarar específicamente que la firma puede ser digital, es decir, que puede servir el acto administrativo normal que habilita para firmar.

-Renato: si alcancé a entender un poco, lo importante de esa habilitación del Ministro de fe, es lo siguiente: uno, es personal, es al RUT tanto, funcionario tanto, al e-mail tanto, que es el Jefe de División que va a hacer tal actuación administrativa, no hay algo

genérico. Dos, que es para el uso de certificados digitales, solamente, es para el uso de la herramienta que va a respaldar la integridad, autenticidad y no repudio, con documento electrónico. Por eso se habla de certificados digitales, es PKI, autenticación robusta y criptográfica, no para otro tipo de habilitación. Entonces, si un funcionario va a entrar en las mañanas al servicio, y el reloj control le lee la huella dactilar, esa claramente no es una actuación potestativa y lo puede definir el área de recursos humanos del servicio público. Está restringido el uso de PKI para manifestar voluntad jurídica, y lo primero que tiene que verificar el Ministro de fe, aparte, de que el tipo sea funcionario a la fecha, es que también sea poseedor jurídicamente o potestativamente de la capacidad de firmar y remendar al servicio. Con todo respeto a los conserjes, a los auxiliares, no firman a nombre del servicio, no podría un Ministro de fe emitirles un certificado digital.

Con esto quiero decir que la herramienta de firmado criptográfica hay que cuidarla. No todos los funcionarios de un servicio, por si, deben tener esta herramienta de firmado, solo aquellos que potestativamente vayan a representar al servicio en actuaciones administrativas, sobre todo en el marco de los procedimientos. Eso también es un criterio clave.

-Roxana: En el caso nuestro solo se inicia un proceso de emisión de certificado si es que tiene una resolución habilitante del Jefe de Servicio, si no, no es posible avanzar. Bueno, Rafael Del Campo consulta: ¿podría el reglamento de la Ley de Transformación Digital hacer extensivo, por defecto, el convenio de MINSEGPRES con todos los servicios públicos, sin que cada uno de los servicios deba suscribirlo, para fines de usar el sistema de certificación?

-Renato: (01:10:11) El reglamento de la Ley 19.880 y después de la 21.180. Habría que ver qué reglamento, porque no tengo claro bien en la reglamentación cual usar. A ver, viene la reglamentación de interoperabilidad, la reglamentación de plataforma, la reglamentación de las direcciones para notificaciones. No sé si hay en el marco legal reglamentación de autenticación, tengo la duda, Rafael. Si lo hubiera, creo que no, porque ese es el tema: hay que buscar cuál es la espalda legal que permitió la norma reglamentaria de detalle, y no lo veo, no lo tengo en mente en este minuto.

-Rafael: Mi referencia es a lo que tú dijiste al comienzo de que debía existir cooperación entre los órganos del Estado, y en ese marco, ¿por qué no facilitamos que se dé por suscrito el convenio entre el MINSEGPRES y todas las entidades públicas?

-Renato: Perfecto, la habilitación para esta colaboración obligatoria. Ojo, dentro de los principios que inspiran el nuevo procedimiento también se habla de la cooperación. Expresamente, por ahí podría ser, en el artículo 16° a nivel de los principios se habla de la

cooperación, pero en el juramento legal anterior está la Ley General de Base de la Administración del Estado, que dice que todos los servicios tienen que compartir recursos. Yo sumo esa ley general, más esta ley, este principio de la Ley de Transformación digital, incorporado el procedimiento administrativo. Ojo, que es importante, lo que se modernizó ahora son los procedimientos administrativos de la Ley 19.880, si me incorpora este principio de cooperación como fundante, podríamos intentar una construcción reglamentaria de detalle, a raíz de la materialización de este principio que ahora es obligación legal, un supuesto de base. Por ahí podríamos buscar una opción para la reglamentación, pero los convenios están estandarizados, por eso se los voy a enviar para que ustedes se los distribuyan. Es un documento público.

-Claudio Delgado: Renato, ¿puedo hacer un comentario respecto a eso? Cuando estábamos trabajando hace unos tres años con Andrés en estos temas, una de las cosas muy importantes que tiene el Convenio con SEGPRES es traspasar las políticas y prácticas de certificación hacia los órganos del Estado, porque se tiene que cumplir cierta formalidad, tanto en la nominación de los ministros de fe, la habilitación de los servicios y en el proceso de certificación. Se buscó a través de Clave Única de tener un registro "presencial" de la persona y después la habilitación del cargo a través del Ministro de fe. Entonces también, va muy enlazado todo lo que son las políticas y prácticas de certificación con el convenio, para que el órgano del Estado no se "arranque con los tarros".
-Renato: (01:12:55) Muy bueno el aporte. Primero, efectivamente el convenio que se está usando ahora es el mismo que desarrolló Andrés en su minuto, cuando él estaba en MINSEGPRES. No le han alterado ni un párrafo, por consecuencia la lógica técnica y jurídica sigue. Segundo, ¿qué son las prácticas de certificación? Son la base regulatoria, reglamentaria administrativa, de todos los procesos tecnológicos. Lo que ahí está definido, es lo que manda después a los operadores electrónicos y digitales. Impuestos Internos tiene sus propias prácticas de certificación digital, que es un documento, un mamotreto que explica los flujos, las competencias, así que muy bien. Y tercero, las políticas de MINSEGPRES o las prácticas de identificación están en la página web de MINSEGPRES, las puedes bajar, lo que pasa es que es una política interna definida sólo para los funcionarios de MINSEGPRES y ahora se hizo extensiva por la vía del convenio como modelo a implementar para estandarizarla al resto de los servicios públicos. Con eso los servicios públicos evitan tener que construir sus propias prácticas de certificación.

No alcancé a hablar del artículo 10 que dice que cada servicio público tiene que reglamentar en detalle toda esta implementación y no lo están haciendo los servicios públicos, ahí están en falta. Salvo Impuestos Internos que tiene un oficio Circular 13. Están en falta porque, ojo, esto ha pasado muy rápido. Roxana, ¿ustedes también lo tienen?

-Roxana: Sí, lo tenemos como procedimiento aprobado. También Claudio Delgado nos aclara que la Armada usa firma SEGPRES.

-José Inostroza: Bueno, yo agradezco mucho a Renato que nos dé seguridad a la mayoría de las personas, porque efectivamente siempre han surgido voces, y yo creo que me incluyo en algún minuto, de temprana ignorancia en estas materias, respecto a la robustez del sistema, etc. Entonces, creo que es muy importante, porque efectivamente al momento de empezar a instalar estas soluciones surgen muchas dudas y lo que está diciendo Renato es muy potente: "esto está operando, está funcionando, tenemos una historia, etc." No obstante y considerando mi pasado en políticas públicas en el gobierno, hay algo que me preocupa y que tiene que ver con lo que se señaló recién respecto a la revocación de los certificados en el sistema público. En Hacienda, estuvo con nosotros el que era director de Gobierno Digital en España y nos relató, a propósito de temas de Clave Única y sistemas de autenticación, un sistema muy extenso, muy profundo, que quedé muy asustado respecto de un directorio de funcionarios públicos, asociados a funcionalidades, a representación legal o no, y qué funciones y certificados de Firma Electrónica. Era muy impresionante, nos mostró: "yo tengo un sistema donde tengo una codificación asociada al ministerio, a mi división y a mi puesto". Eran casi tres niveles y su nombre y la funcionalidad que ellos le daban a eso. Tienen una claridad certera respecto de quien podía firmar y quien no, por cuánto tiempo. Entonces el sistema de revocaciones era muy automático. Había un responsable, que era una especie de conservador de funcionarios públicos y sus capacidades de firma, y se revocaba automáticamente para una función u otra. Una persona tenía la posibilidad de firmar en cuanto funcionario público, en cuanto a representante eventualmente de una empresa. Ellos hicieron todo un sistema para poder aclarar esto. Yo quedé muy asustado, porque sentí que eso estaba muy lejos de las capacidades nacionales, digamos, en todo orden de cosas, no sólo tecnológicas, sino sobre todo organizativa. De hecho en Chile no tenemos capacidad siquiera de saber quiénes son los funcionarios públicos. Menos vamos a tener un directorio de los firmantes.

Ahora también, varios dijeron: "eso es exagerado, los españoles son eventualmente muy burocráticos, no tiene ninguna importancia". Pero me quedé con la duda. En Uruguay me dicen: "acá pasa lo mismo". Son dos países que están muy arriba en los niveles de clasificación de Gobierno Digital de la OECD. España está en el número 7 a nivel mundial y Uruguay, no sé, estará en el número 12 o 15. Entonces si ellos lo hacen, yo me pregunto humildemente, ¿no debiéramos avanzar hacia eso? No digo que sin eso no podamos funcionar, sólo digo que prudencialmente, cuando esto sea muy masivo y haya cientos de

miles de funcionarios firmando, millones de documentos, ¿no será bueno en los próximos años tener un directorio de esa naturaleza?

-Renato: Una contra pregunta José, ¿en qué lugar está Chile en ese índice?

-José: Es de los últimos de la OECD. Yo creo que estamos en el 25 porque no hay 30 países.

-Renato: la pregunta me parece tremendamente interesante, porque da en el clavo ¿de qué se trata esto? Esto tiene tres capas, tres lecturas: la de gestión administrativa de respaldo institucional, la tecnológica y la jurídica. Quedémonos en la primera, ¿de qué se trata? De emitir certificados digitales para respaldar la identidad del funcionario, o sea, de decirle a los ciudadanos o a las contrapartes de los otros servicios públicos: "este señor que está firmando es el Jefe de la División Administrativa de… la municipalidad, de la Contraloría General de la República, y la imagen. Entonces, eso yo lo puedo traquear y lo puedo, efectivamente, administrar. Si sucede que ese funcionario fue dado de baja por un requerimiento, claramente revocar un certificado es cuestión de segundos, ¿te fijas?

Lo que estamos hablando es ¿cómo ordenamos la gestión de la administración? No hablemos de certificados digitales, hoy en día cada servicio público emite un carnet de plástico, que dice de qué servicio eres, y esta es la misma lógica. Pero en materia de certificados digitales, hay un elemento que falta, que no se ha explicado: la autenticación de un signatario funcionario tiene que ser validada en una cadena de confianza hacia arriba, por eso la estructura piramidal. Entonces si el organismo acreditador es la ley o es el Estado y va a ser en definitiva, porque hay que definirlo, no hay uno central en este minuto. Está Economía, pero sólo para el sector privado. Si definimos un organismo central de gestión digital, de administración de seguridad en esta cadena de confianza, en el segundo nivel, si un Ministro de fe. En el primer nivel está el acreditador, en segundo nivel está el servicio público, su Ministro de fe, y en el tercer nivel los funcionarios. Si este Ministro de fe, habilitó a un funcionario Jefe de División de tal servicio, jefe de compras, adquisición, administrativo, y la persona sale, inmediatamente eso se puede traquear en cuestión de segundos. Los sistemas funcionan automáticamente y la cadena de confianza llega arriba.

(01:20:17) Por otro lado, yo proveedor del Estado, tercer nivel, recibo un documento firmado por este señor signatario de adquisiciones de un servicio público, y desconfío, debo poder, técnicamente, también en cuestión de minutos, porque eso lo permite la PKI, escalar. Voy al servicio público que sea y no me dice nada, escalo al organismo acreditador y ahí en un sitio web tiene que estar lo que se llama el CRL, si los certificados no han sido revocados o llamadas públicas vigentes. Yo puedo con el número de serie del documento

llegar hasta arriba, debo poder verificar la identidad del tipo que está firmando. Esto está implementado, y esta es la jerarquía de confianza de las infraestructuras de llave pública.

-Roxana: Hay un uso que yo veo más allá. Y perdón que te interrumpa en esto. Dentro de los problemas que tenemos en el mundo de la información, no tiene que ver con la ley ni con las condiciones técnicas. Tenemos problemas con todo lo que es el ámbito de la preservación digital, y que es un ámbito post, cuando ya ha terminado el ciclo de tramitación, el ciclo vital de un documento. Los prestadores tienen la obligación de resguardar los certificados por seis años. Y en el fondo, una parte importante va a tener que ser traspasado al Archivo Nacional. El tener un instrumento como ese permite tener un validador, porque o sino el Conservador del Archivo no va a tener contra qué validar. Entonces es un instrumento muy útil, porque de alguna manera va a certificar aún cuando el certificador original no mantenga el certificado, va a poder tener un lugar para contrarrestar. Y eso es muy importante, para el proceso de preservación histórico, que es un comentario que les quería hacer, porque nunca se mira esta parte. Y la segunda parte que es muy clave, y que tampoco tiene que ver con la ley, tiene que ver con las condiciones tecnológicas y es que el actual estatus de la firma que tenemos en Chile no se considera longeva. Por lo tanto, cuando en algún momento los documentos firmados digitalmente, deban ser migrados de formato, vamos a perder esa relación con los certificados. Entonces hay dos problemas que son graves, pero no son para el actuar de la administración hoy, sino para la responsabilidad del archivo.

-Renato: Con todo el cariño que te tengo, voy a discrepar o intentar aclarar lo que acabas de decir. Primero, los certificados digitales en el mundo privado, envié un comentario en el chat, efectivamente respaldan la identidad de personas naturales. En el sector público respaldan exactamente lo mismo, la identidad de una persona natural con RUT, con e-mail, pero tanto en cuanto funcionario de un servicio público, por eso es que el servicio público puede gestionar y revocar el certificado de autenticación.

Segundo, los certificados digitales tienen un plazo temporal de vigencia: un año, dos años, tres años. Esa definición no es legal, no es normativa, es operatoria, es tecnológica y es comercial. O sea, una empresa certificadora puede emitir un certificado por 10, 15 o 20 años. Técnicamente, los estándares de PKI sugieren que no es conveniente, por la posible alteración del rol, de la competencia, del rol contractual, de la persona que fue respaldada…

¿A qué viene el punto? En este minuto, no hay un discurso, no hay un relato coherente entre lo jurídico y lo técnico en la vigencia del certificado, quiero ser bien claro…

-Roxana: yo no estoy hablando de la vigencia del certificado…

-Renato: ¿Por qué lo digo? Cuando tú dices que la empresa chilena tiene que guardar el certificado por 6 años, no es correcto…

-Roxana: Así estaba en el reglamento.

-Renato: Eso es lo que quiero tratar de precisar. No porque esté en el reglamento significa que sea claro. Revocado un certificado o caducado por plazo un certificado, no hay más respaldo de la identidad digital del funcionario. Si yo firmé un 1 de enero del 2001 y quiero verificar la validez de la firma el 1 de enero del 2014, cuando voy a verificar las propiedades de la firma, me va a decir firma inválida, certificado revocado. y en ese entonces no puedo ir ya a la entidad certificadora a pedirle: "oye, pero si hace 14 años yo firmé con tu software, dime que fue firma válida" No es el rol, ni legal, ni reglamentario de la certificación.

-Roxana: Por eso te digo, ese es el problema que tenemos. Lo tenemos clarísimo. El problema que tenemos queda más claro con un ejemplo que yo siempre pongo: si yo Conservador, tengo que firmar como copia fiel un documento, por ejemplo que firmó O'Higgins, si alguien me lo quiere cuestionar, tengo un perito calígrafo. Lo que estamos perdiendo es el perito. Porque ese es un problema que va a tener el Conservador al querer autentificar. ¿Existió o no existió? Y al tener instrumentos como el que menciona José, permitiría mantener un control de identidad. Ese era el problema: pierdo el perito y al perder el perito, el Conservador queda en un espacio muy feble, digamos, porque no tiene la certeza. Ese es el problema.

-Renato: Pero hay una solución. Hay una solución jurídica, hay un criterio jurídico que se puede recoger. Si yo firmé en el Archivo Judicial, firmé un documento el 1 de enero del 2010, caduca el mismo documento con firma inválida el 1 de enero del 2014, tres años después, así de simple. En algún momento alguien firmó y jurídicamente existe el tema del principio de prueba por escrito. Yo puedo intentar, no tengo un perito calígrafo, pero tengo un perito informático. Y ese peritaje informático podrá determinar que efectivamente fue firmado oportunamente por esa empresa. Hay mecanismos colaterales que podrían colaborar al reconocimiento de un documento, puedo citar al reconocimiento de firma al que firmó en su momento, ¿te fijas?, hay andamiaje jurídico que podrías recoger para intentar validar.

-Roxana: Sí, pero todavía es bien gris ese problema, porque no lo tenemos encima, porque lo vamos a empezar a tener en los próximos 5 o 10 años, pero en este momento estamos advirtiendo el problema y debe conducir a algún tipo de solución. Ya sea que haya un repositorio de firma, ya sea que haya un maestro de autoridades del Estado, lo que sea, pero hay que generar las certezas para quien está certificando un documento como copia

fiel, que pueda hacerlo bajo algún instrumento que lo apoye. En este caso, el Conservador, tiene el original. Ahora, podrían cuestionar el original, evidentemente, pero eso ya es entrar a un tema que podría ser más del ámbito del fraude, digamos.

-Pilar Díaz: (01:28:24) Bueno, este tema es bien complejo, y en términos generales, nosotros, los del Proyecto de Modernización del Archivo Nacional, tuvimos esta asesoría internacional. De hecho va a quedar un documento comparativo: diferentes países han adoptado diferentes soluciones para enfrentarlo. El tema es que efectivamente no vamos a encontrar la solución ideal y no podemos quedarnos inmovilizados a esperar la solución ideal. Porque efectivamente la tecnología va a ir evolucionando a lo largo del tiempo y a lo mejor en 5 años más encontramos la solución de un estándar para todo el mundo, pero en este caso, en este momento, cada país está solucionando en su propia forma.

Ahora, en términos reales y esto se lo escuché a José, hace muchos años atrás y en su momento no me pareció, pero ahora creo que tiene toda la razón. Él decía que al electrónico no hay que pedirle más que al papel, o sea, por qué le pedimos más certeza al electrónico cuando al papel tampoco es que seamos tan exigentes con ciertos ámbitos. En los documentos que por sí entran al Archivo Nacional, nosotros pensamos que es menester de la institución productora corroborar y asegurarse que esos documentos que entran, son válidos, han sido emitidos correctamente y firmados por quien corresponde. Eso es parte de la gestión documental de la propia institución, por tanto cuando esos documentos ingresan al Archivo Nacional vía transferencia electrónica, se presupone, porque para eso está el Archivo, y a partir de ahí, que esos documentos son válidos. Fueron firmados por quién corresponde y el archivo está a cargo de garantizar la custodia y que las migraciones que se realicen de formato, etc. vayan dejando registro de eso. Ya, en ese sentido, de hecho, los coreanos, si no me equivoco, lo que hacían, era que en el fondo al documento que ingresaba le colocaban un sello especial y a partir de ahí en 5, 10, 15, 20 años más, si estaba con ese sello, se daba por hecho de que era válido y de que fue firmado por quien correspondía. Entonces, efectivamente es un tema que cada país tiene que asumir de acuerdo a sus posibilidades y también apoyado siempre por la normativa. O sea, si la normativa indica y garantiza que los archivos, documentos, que son recibidos por el Archivo Nacional y fueron firmados en su momento. En términos reales hoy en día el Conservador del Archivo Nacional no garantiza que los documentos que recibe, no revisa firma por firma, no hace ese trabajo tampoco tan minucioso. Lo que sí creo que es importante y eso es parte de lo que se está haciendo en el repositorio, la confianza que se está generando es por el OAIS, ¿cierto? A través de los metadatos y los metadatos especiales de preservación digital, los PREMIS, los METS, se están consignando los documentos que efectivamente vienen con firma digital, e inmediatamente el sistema va captando y heredando esa información. Efectivamente, no es la solución ideal, pero es un

paso más hasta que vayamos descubriendo cuál es el tema. Ahora, yo creo que el concepto clave es que el Archivo es el custodio de la información que le es entregada, transferida, ¿no es cierto?, por las instituciones productoras, y son ellas, las instituciones públicas las que tienen que asegurarse que su gestión fue bien realizada y firmó quien tiene que firmar. Ese es mi aporte ahora e insisto, es un tema magno, no es menor, pero yo creo que tenemos que afirmarnos en el rol del Archivo Nacional en este caso.

-Macarena: (01:32:21) Siguiendo la línea de lo que mencionaba Pilar y sumándome también al comentario de José, respecto a que no le podemos pedir más a lo tecnológico que al papel, creo que también hay que tener claridad cómo funcionan los servicios públicos hoy día. Y en el funcionamiento de los servicios, hay que hacer buena conciencia respecto a lo que significa la existencia de una Firma Electrónica hoy día. La contratación de un funcionario está radicada en el área de recursos humanos. El concepto del dispositivo tecnológico, del token, está radicado en tecnología. El concepto del Ministro de fe, probablemente está radicado a lo mejor en el Centro de Documentación o en alguna otra parte, tal vez en Fiscalía. ¿Cómo logramos que esos tres entes, dentro de un mismo servicio público, estén coordinados, de manera de que cuando un contrato de alguien o una persona deja de funcionar como cierto rol y empieza a funcionar como otro, que esos tres entes se coordinen y efectivamente el token se inhabilite, la persona cambie su forma de contratación, y el Ministro de fe lo deshabilite. Si no existe esa conciencia, da lo mismo lo que diga la ley, da lo mismo lo que diga nuestra teoría, eso no va a funcionar. Creo que es muy importante el incentivar esta conciencia respecto a la Firma Electrónica. Hoy yo no sé quienes realmente certifican la firma manuscrita, si alguien saca un documento manuscrito y a lo mejor está falsificando la firma de algún funcionario, ¿tenemos realmente la forma de comprobarlo? Probablemente, tampoco la tenemos. Entonces tenemos que pensar en qué robustecer en los servicios, y entre los servicios, porque tenemos que recordar que todas las contrataciones se hacen a través de SIAPER, que lo maneja la Contraloría General de la República. Y por lo tanto, si queremos revocar un certificado, o tener un historial de cuáles son los roles que ha tenido esa persona, esa información se podría contrastar con lo que dice SIAPER, por ejemplo, independiente de la responsabilidad que le cabe a los servicios públicos de hacer eso por cada uno de sus funcionarios. Creo que no solamente tenemos que ver la parte legal, sino que también ver la forma práctica en que esto tiene que funcionar de buena manera y que los servicios deben tener recomendaciones, hechas por los reglamentos, respecto a cómo se tienen que autenticar los funcionarios públicos y los roles que les corresponden en cada firma.

-Renato: Dos comentarios breves. Sobre lo último, completamente de acuerdo, salvo que SIAPER, más que verificar identidades, administran y manejan documentos concretos. Entonces la pega de sacar el dato o data de quién fue el funcionario es una pega adicional.

Ellos toman o no toman razón del documento, hacen gestión documental, lo veo un poco lejano. Pero la Contraloría tiene un rol clave, creo que lo conversamos el otro día, y no sé si tiene conciencia de este rol clave en la habilitación del flujo documental.

(01:35:52) Quiero volver a lo que decía Pilar, y lo comentó José por ahí en el recto sentido, y lo comparto. Toda esta implementación tecnológica no significa hacer tabla raza de las normas legales de derecho público que existen a esta fecha. Y si el Archivo Nacional tiene un rol asignado por su ley orgánica o por leyes especiales, de garante de la autenticidad de documentos que archivó para los próximos años, eso prima jurídicamente, por sobre la limitación o las restricciones tecnológicas. Roxana mencionó el Conservador. Si el Conservador tiene que guardar escrituras de propiedades inscritas por 25, 30, 40 años, para hacer los informes, los estudios de título, los certificados de dominio vigente, y el certificado caduca el año 3, el Conservador tuvo un rol potestativo jurídico de Derecho Público que subsiste. Él va a decir:"yo desde el día 1 y hasta el año 3, recibí dicho documento. Y efectivamente, cuando ya no hay Firma Electrónica válida para el documento en sí mismo, soy Conservador. Es mi potestad y de allí en adelante, respaldo la integridad de autenticación de esa escritura pública que incorporé a mi registro en su minuto". Los notarios, tienen un rol exactamente similar desde el punto de vista de resguardo de los documentos, más allá de las caducidades temporales. Y ¿Por qué digo esto? Porque es complejo para el otro escenario, por una propuesta que hay en este minuto, en el sentido de traspasar toda esta gestión al Servicio de Registro Civil, pensando que solo es una gestión tecnológica. El que todos los registros de poder, es que todas las hipotecas, que todos los documentos pasen al Registro Civil, no van de la mano solamente porque tenga un buen desarrollo su plataforma tecnológica. Requiere una definición de competencias de Derecho Público, que son éstas que estamos viendo. Así que lo que ha hecho el Archivo y la postura de Pilar Díaz, indican que habría una solución propietaria nacional. Creo que es la perspectiva jurídica la que puede hacer coincidir estas normas especiales de facilitación de gestión documental con las normas potestativas de Derecho Público que no caducan y se mantienen vigentes.

-Roxana: Quiero avanzar pues hay muchas preguntas. J. Contreras que nos comenta que el sellado de tiempo es muy importante, ya que indica exactamente cuándo se ha firmado un documento, y usa la misma tecnología. También señala que el sellado de tiempo es gratis en la actualidad, pues viene incluido en la venta de los certificados. Francisca Tagle indica que existe sellado de tiempo y lo asimila a la protocolización de documentos privados. Luis Fuentes, hace una pregunta: ¿qué te parece la incorporación de un certificado de Firma Electrónica Avanzada en la próxima cédula de identidad?

-Renato: Me parece espectacular, pero ese tema, con todo respeto, es de la época de Claudio Orrego. O sea, más que una Firma Electrónica Avanzada, lo que se incorpora, cuando los documentos tengan un chip, es tener el certificado habilitante para que un lector pueda leer la cédula y yo pueda respaldar la identidad. El tema se descartó en su minuto, entiendo por los costos que involucra desarrollar un chip para incorporarlo al carnet de identidad. Pero la propuesta, está implementada en algunos países, no recuerdo cuales. Incluso, en algún minuto se empezó a vender en el comercio computadores con lector de chip para leer certificados digitales y te estoy hablando del año 2000. Conceptualmente lo comparto: andar trayendo mi herramienta de firmado no en un token, no en un computador, no en una nube, no en un servidor HCM, sino que andar portándola en mi carnet y eso masificaría el tema de la autenticación segura, pero el problema son los costos y la implementación.

-Roxana: Macarena nos pregunta, desde la perspectiva de una persona natural, haciendo trámites frente a un servicio público, ¿en qué tipo de procedimientos se le podría forzar a contar con FEA y por ende incorporar un costo adicional en el trámite?

-Renato: (01:40:37) Ninguno, te explico por qué. La única barrera de entrada FEA, hablo de los certificados digitales a los ciudadanos. La FEA es obligatoria, artículo 4°, solamente para los funcionarios públicos. Eso dice el artículo 4°. Al otro lado, primero, yo le puedo agregar otro mecanismo de autenticación, pero estamos esperando qué va a decir el reglamento. Pero obligar a pagar un certificado digital al ciudadano para interactuar con la administración del Estado, por distintos aspectos regulatorios no corresponde. Es una carga adicional que la ley no establece en ninguna parte. Incluso es más, lo que la filosofía de la reforma de la gestión digital, es todo lo contrario. La filosofía dice: usa toda la implementación tecnológica que se pueda y se regule. Y si te encuentras con ciudadanos que no son capaces, por sus capacidades tecnológicas de operar digitalmente, vuelve al papel, la perspectiva es toda lo contraria. Entonces, obligar, per se, sin ninguna justificación a que el ciudadano tenga certificados digitales, absolutamente descartado. Ahora bien, la autenticación tiene que ser segura y robusta. Y si quiero que un ciudadano ingrese a ser notificado de todas las resoluciones de la administración del Estado, a una casilla, claramente la autenticación de esa casilla tiene que tener estándares tecnológicos robustos y altos, pero ese es otro problema. Ahí el ciudadano no va a poder decir: “no es que no quiero usar dos claves, es que no quiero que me llegue un mensaje al celular. Es que no quiero tener tres mecanismos de autenticación. Eso tampoco lo puede decir”. Pero por un tema de seguridad de gestión de la información, que también está considerado dentro de la modificación. No olvidemos nunca que hay un artículo 19 bis, que se refiere a las plataformas, y dice que todas las plataformas tienen que ser seguras, íntegras, interoperables y ciber seguras. Entonces si para una plataforma se define cierto estándar

de autenticación para ingresar, un ciudadano no va a poder decir: “es que no me gusta”. No, la verdad es que los estándares de gestión segura te obligan a implementar la autenticación robusta. Pero exigencia de certificado digital en la otra punta, en el ciudadano para interactuar con la administración, no hay exigencia legal hasta esta fecha.

-Roxana: (01:43:00) Lamentablemente ha terminado el tiempo. Agradecer a Renato por su generosidad en compartir su conocimiento. Excelente presentación. Los dejamos invitados para nuestro próximo coloquio sobre Inteligencia Artificial, el próximo viernes, con Sebastián Ríos de la Facultad de Ciencias Físicas y Matemáticas de la U. de Chile.