autelsi

Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información

SERVICIOS DE CONFIANZA

En el marco de la situación actual provocada por la Covid-19

JULIO 2020

SERVICIOS DE CONFIANZA

En el contexto actual, provocado por la crisis del Covid-19, y con el fin de encontrar soluciones que permitan mantener la continuidad de los negocios, hemos sido testigos de la implantación, por parte de las organizaciones, de multitud de medidas o soluciones tecnológicas dirigidas a garantizar la seguridad de la actividad, respetando al mismo tiempo los derechos de los trabajadores, usuarios y consumidores. Entre esas medidas podemos destacar la implantación del teletrabajo en prácticamente todos los ámbitos y, en muchos casos, la digitalización de los procesos empresariales.

También las organizaciones han ido adaptando su actividad y la gestión de sus procesos internos a las necesidades provocadas por el estado de alarma y han desarrollado modalidades de servicios en línea o a distancia que antes de la pandemia no tenían implementadas. Servicios y procesos que exigen de garantías de seguridad en las transacciones y procesos *end-to-end*.

Un hecho destacable también es el incremento considerable de las operaciones telemáticas y, en menor grado, el uso de la firma electrónica y de los servicios de confianza.

Recordemos que los **servicios electrónicos de confianza**, tal y como se definen en el Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE **(Reglamento eIDAS)** son el aspecto principal del mercado único digital que pretende eliminar las barreras al comercio electrónico y a todo tipo de transacciones electrónicas entre los diferentes estados, englobando los servicios relativos a la creación, verificación y validación de firmas electrónicas, sellos electrónicos, o certificados para la autenticación de sitios web, entre otros. Sin duda alguna, uno de los aspectos más destacados del Reglamento eIDAS es la **creación de los prestadores cualificados de servicios de confianza** (en su acepción inglesa, los Service Trust Providers -TSP´s).

En el ámbito del derecho interno, desde el pasado día 19 de febrero de 2020 se encuentra en tramitación el **Proyecto de Ley Reguladora de Determinados Aspectos de los Servicios Electrónicos de Confianza** que, derogando la vigente **Ley 59/2003, de 19 de diciembre, de firma electrónica**, regulará aquellos aspectos que el Reglamento eIDAS deja en manos de los Estados Miembros y eliminará aquellas incompatibilidades entre la normativa europea y la actual regulación española de firma electrónica.

En cuanto al incremento de la utilización de los servicios de confianza, el balance de quien los han implementado es que les ha permitido que las interacciones entre las empresas, los ciudadanos y la Administración Pública, sean más seguras. Esta seguridad que aporta el uso

de los servicios de confianza no solo es técnica, mitigando los riesgos de exposición a la disponibilidad de los servicios, la integridad o la confidencialidad de la información, sino jurídica, al dotar de garantías eficaces para acreditar fehacientemente la identificación de los sujetos que intervienen en las operaciones telemáticas.

No obstante, en este contexto de cambio normativo y empresarial, es en el que el uso de los servicios de confianza ha puesto en evidencia determinadas situaciones que merecen análisis y respuesta de los agentes intervinientes. A modo de ejemplo: la falta de conocimiento o entendimiento de parte de la población del contexto de confianza digital y de los elementos que en ella intervienen como ¿qué es un certificado electrónico?, la posible desconfianza en su uso, la falta de medios informáticos, el manejo del mismo, los tipos de firma digital, la validez de las misma, el apoderamiento de uso o seguridad que aporta, entre otros.

En definitiva, en el presente trabajo queremos destacar que todo este contexto sobrevenido a raíz de la pandemia Covid19, hace necesario que reflexionemos sobre los cambios que deben acometerse en las organizaciones para adaptar nuestras organizaciones y proceder a analizar los posibles riesgos que estos cambios han o pueden generar, ya sean técnicos, jurídicos u organizacionales y como los servicios de confianza pueden contribuir a la mitigación de estos riesgos. Entre algunos riesgos a destacar podemos citar aquellos derivados de:

- La Ciberseguridad desde el propio hogar y dispositivos, redes de conexión.
- La Seguridad Sanitaria y la aplicación de las medidas adoptadas por el COVID19.
- La seguridad Laboral al trasladarse el puesto de trabajo al hogar.
- La seguridad jurídica de las transacciones y procesos, sus trámites.
- La seguridad de la información empresarial para poder garantizar la continuidad del negocio, la privacidad y el uso indebido de los activos de información.
- El mantenimiento de la cultura de “Compliance” y lo que implica en el Cumplimiento, Compromisos y Comportamiento
- La Interoperabilidad entre Plataformas, Actores, Herramientas, Soluciones, etc.
- La Seguridad Operativa en si misma al afectar a cambios de Procesos internos.
- La Homologación, acreditación, certificación o calificación de Protocolos, Servicios, Productos, etc.
- La Auditoría y Control de Procesos internos.
- La propia Gestión de Recursos Humanos.

Debemos destacar, por último, como en este contexto de cambio se hace clave crear una cultura, estrategia y mecanismos de resiliencia organizacional y social sostenible en el tiempo que nos haga estar preparados para responder, recuperar y superar los nuevos riesgos, amenazas y sus consecuencias.

Por ello creemos que los análisis de debilidades, amenazas, fortalezas y oportunidades (DAFO) que incluimos a continuación pueden dar una visión práctica y útil para buscar soluciones habida cuenta que, en nuestra opinión, ahora los servicios de confianza digital son más esenciales que nunca.

ANÁLISIS DAFO: LA SITUACION ACTUAL (COVID -19): NECESIDADES DE LA SOCIEDAD Y LOS SERVICIOS DE CONFIANZA

En este apartado, examinamos cuál es la situación actual de la sociedad, las organizaciones y las necesidades que se han visto incrementadas como consecuencia de la COVID-19 y su perspectiva ante el uso de los servicios de confianza.

En este sentido, se analizan algunas de las principales debilidades, amenazas, fortalezas y oportunidades desde la perspectiva actual de servicios y actividades y la implantación y uso de los Servicios de Confianza:

DEBILIDADES

- Imposibilidad de acceso al dispositivo en el que está instalado el certificado por encontrarse instalado únicamente en los ordenadores de mesa.
- Falta de prevención y planificación frente a emergencias que puedan suponer la adopción inmediata de este tipo de servicios.
- Ausencia de formación en tecnología (configuraciones, actualizaciones de Java, sistemas operativos,) y, en consecuencia, inseguridad en su uso.
- Dificultades para visualizar contenido del acto jurídico que se está firmando (como, por ejemplo, firma de contratos en tabletas, TPVs digitales)
- Almacenamiento de la información firmada con el certificado electrónico.

AMENAZAS

- Desconocimiento sobre el uso de los certificados y forma de proteger las claves
- Uso por diferentes personas del mismo certificado
- Riesgo de robo o pérdida del dispositivo en el que está instalado el certificado
- Riesgos de ciberataques que comprometan la información que se aloja electrónicamente.
- Pérdida de oportunidades por la falta de implantación de los servicios de confianza.

FORTALEZAS

- Digitalización de la prestación de servicios por las compañías y las administraciones públicas.
- Agilización de los procesos para recabar firmas en documentos con varios sujetos intervinientes, por ejemplo, actas de Consejo de Administración.
- Seguridad jurídica sobre el contenido y firmante, en función del certificado que se implante
- Tecnología madura y segura

  Mantener la seguridad jurídica durante el estado de alarma.

OPORTUNIDADES

- Reducción de costes y tiempo de gestión
- Agilización de los procesos de digitalización de las empresas en el proceso de confinamiento derivado del Covid.
- Mejora de la conciliación familiar, se ha potenciado el teletrabajo.
- Nuevos sistemas de identificación sin necesidad de presencia física.

  Fomento y agilización del acceso a nuevos mercados, especialmente el entorno online.

En resumen, podemos decir que:

DEBILIDADES. Las principales debilidades que encontraríamos a nivel social se encontraría la **falta de previsión** por la sociedad y las organizaciones a la hora de contar con servicios electrónicos de confianza que ya se encuentran previamente implantados en las compañías, de forma tal que se **imposibilita el acceso a los dispositivos** en los que se encuentran instalados, por ejemplo, al instalarse únicamente en ordenadores de mesa. Asimismo, la **ausencia de formación tecnológica** también ha provocado cierto caos organizativo a la hora de conocer, por ejemplo, el lugar de **almacenamiento** de los documentos firmados o poder **visualizar de forma íntegra el documento** que se está firmando electrónicamente.

AMENAZAS. Como principales amenazas se podrían citar entre otras las derivadas **del uso incorrecto de los certificados** electrónicos por diferentes personas, así como la posible **pérdida del control del certificado** por ciber-ataques o la pérdida de los dispositivos en los que se encuentran instalados los certificados electrónicos.

FORTALEZAS. Entre las fortalezas que aporta la implantación de certificado electrónicos destacamos, sin lugar a duda, que permitirá la **digitalización** de las compañías, a través de la **agilización de los procesos de firma** de documentos, entre otros, contratos mercantiles o financieros y la seguridad jurídica con la que contarían las Organizaciones tanto a nivel jurídico como técnico por el uso de certificados electrónicos válidos.

OPORTUNIDADES. La situación vivida en los últimos meses ha puesto de manifiesto que la implantación y uso de certificados electrónicos permite **agilizar procesos de digitalización** de las empresas, así como la **reducción de tiempos de gestión**, de costes y el **aumento de las posibilidades de acceso a otros mercados** que tradicionalmente requerían una presencia física para el desarrollo de nuevos negocios.

ANÁLISIS DAFO: SERVICIOS DE CONFIANZA PSC /TSPS

Con la actual situación provocada por la COVID-19 se ha puesto de manifiesto el papel fundamental que juegan los Prestadores de Servicios de Confianza o en su acepción inglesa, los Service Trust Providers (en lo sucesivo, PSC/TSPs) en el desarrollo de la digitalización de la sociedad y la incipiente necesidad de realizar distintas actuaciones y/o negocios jurídicos "a distancia". En este sentido, se analizan algunas de las principales debilidades, amenazas, fortalezas y oportunidades desde la perspectiva de los PSC/TSPs:

DEBILIDADES

- **Falta de cultura** de los tipos y validez legal de los medios de identificación electrónica y/o de firma por parte de los ciudadanos y empresas.
- **Desconfianza de los usuarios** hacia este tipo de tecnología y, que tiene como consecuencia la incertidumbre durante la identificación y/o firma.
- **Complejidad** de tecnología de certificados, y alta dependencia de los PSCs/TSPs
- Instrucciones técnicas de desarrollo legislativo europeo y Nacional **con falta de concreción** y alta dependencia de organismos nacionales competentes para el desarrollo de éstas (videollamada, biometría, etc.) todos los actores involucrados.
- **Coste de implantación** de los mecanismos de autenticación y firma.

AMENAZAS

- **Riesgo por ataques** a los medios de identificación y/o firma, o a los servicios expuestos y por utilización indebida de los mismos
- Diferente grado de aceptación en función del **sector de población**
- **Confusión** entre los distintos tipos de medios de identificación y/o firma y las ventajas e inconvenientes de cada uno
- Mayor **impacto de incidencias** tecnológicas, que pueden afectar a la disponibilidad, confidencialidad, integridad y **privacidad** en los servicios expuestos
- Gran impacto en los servicios de los **desarrollos normativos o legales**.

FORTALEZAS

- **Cercanía** al ciudadano y a la empresa
- **Interoperabilidad** entre los diferentes medios de identificación de todos los países miembros de la UE
- Se establecen **diferentes niveles de identificación**, lo que permite adaptarse a cualquier escenario
- **Homogenización legal** de los tipos de **firma** a nivel europeo y **presunción de veracidad** de la firma electrónica cualificada

Tecnología **madura** y razonablemente **segura**.

OPORTUNIDADES

- Reducción de **costes**, **simplificación**, **optimización** y **automatización** de trámites administrativos y procesos
- Reducción de impacto en medio **ambiente**
- **Transformación digital** de los procesos empresariales y posibilidad de **creación de nuevos servicios**
- **Mercado único digital** que permite el desarrollo de nuevos servicios interoperables

Contribución a minimizar el posible **fraude** en trámites de las Administraciones Públicas y en el ámbito privado.

DEBILIDADES. En primer lugar, como principal debilidad, se ha detectado que en términos generales no existe una amplia cultura sobre los distintos tipos de certificados electrónicos y/o medios de identificación electrónica disponibles, así como la validez jurídica que la legislación otorga a cada uno de ellos. Esta situación provoca cierta **desconfianza** de los usuarios, ya que no conocen la **tecnología** ni las consecuencias derivadas de la utilización de estos mecanismos tecnológicos que en gran medida son percibidos con cierta **complejidad**.

AMENAZAS. Por otra parte, no todas las organizaciones y, en general, la población ha asumido con el mismo **grado de aceptación** el desarrollo y la necesidad de utilización de los certificados electrónicos y sistemas de identificación electrónica. Ello ha podido venir determinado por distintos factores tales como la **confusión** de los diferentes medios de identificación y firma electrónica, el **riesgo de ataques** sobre los propios **certificados / medios de identificación** o bien sobre los servicios expuestos y las consecuencias derivadas de una **utilización indebida** de los mismos que podría afectar a la disponibilidad, confidencialidad, integridad y **privacidad** en los servicios expuestos. Cabe destacar que la **falta de concreción** de los desarrollos normativos o legales ha incrementado esta situación.

FORTALEZAS. Sin perjuicio de lo anterior, existen aspectos positivos que deben ser resaltados en la situación actual, tales como la **cercanía** con la que parte de los ciudadanos perciben estos **servicios**, alto grado de **interoperabilidad** y **consenso** a nivel europeo, **adaptabilidad** de los niveles de identificación en función de las necesidades de los ciudadanos, **homogenización y validez legal** de los efectos jurídicos producidos utilizando ciertos tipos de certificados electrónicos y los servicios asociados a los mismos bajo una **tecnología** razonablemente **segura** y **madura**.

OPORTUNIDADES. El escenario actual constituye un reto para los PSC/TSPs al objeto de alcanzar un alto grado de implantación y **uso** de este tipo de servicios de forma **generalizada** en la población y en las organizaciones. La materialización del despliegue y uso de los certificados / medios de identificación de forma generalizada por parte de los ciudadanos y organizaciones **reducirá costes**, **simplificará procesos** empresariales y administrativos y la tramitación de estos, contribuyendo a la **transformación digital** y a la **reducción de fraudes**. Lo que sin duda favorecerá el **desarrollo** de un **mercado único digital** y de nuevos servicios interoperables asociados. Asimismo, se lograrán **beneficios medioambientales**, reduciendo el uso del papel y ahorro en combustible como consecuencia de la minoración en desplazamientos innecesarios para la realización de gestiones.

CONCLUSIONES FINALES

El uso de servicios de confianza de forma masiva y generalizada aporta seguridad, ventajas para la sociedad y productividad porque facilita la mejora de la simplificación de procesos, la mejora de la seguridad en la prestación de servicios a distancia, la reducción de costes, y la minimización de fraudes. Estamos ante un proceso imparable de transformación digital en un entorno de tecnología que presenta un alto grado de seguridad y madurez.

La actual situación y la crisis provocada por Covid-19 nos ha puesto de relieve la necesidad de transformar digitalmente nuestras organizaciones y mejorar las comunicaciones a distancia.

No obstante, resulta del todo necesario que se mejore el conocimiento de la sociedad sobre el uso, características y seguridad para la adecuada utilización de los servicios de confianza como certificados electrónicos, medios de identificación o servicios de entrega, mejorando la formación tecnológica e incorporando terminología clara y accesible para todos. Entendemos que se precisa una labor de formación, concienciación y pedagogía en el uso de la firma electrónica y los servicios de confianza en las organizaciones públicas y privadas y en la sociedad en general.

En conclusión, poder disponer a nivel europeo de sistemas estándar seguros a nivel jurídico y tecnológico para la identificación de personas y entidades y realización de gestiones con certificados electrónicos, supondrá un gran avance de la sociedad hacia un Mercado Único Digital Europeo que propiciará mayor autonomía para la realización de gestiones y aumentará la competencia, eliminando barreras geográficas.

El cambio que supone la utilización de los servicios de confianza ha venido para quedarse por el valor indudable que aporta. Desde el Grupo de Regulación de Autelsi entendemos que cuanto antes se aceleren los procesos en el uso de los servicios de confianza, se mejorará la seguridad jurídica y tecnológica y se garantizará la competitividad de nuestras empresas en un entorno global.