GUÍA DE LA SOLUCIÓN

besign | Serban Biometrics

SOLUCIÓN DE FIRMA BIOMÉTRICA PARA EL SECTOR FINANCIERO

Optimizando los procesos del negocio a través de la movilidad

>

Un Sector en Evolución

El Mercado Financiero se encuentra en continua evolución. La reducción del número de oficinas debido a la consolidación de las entidades **(36% desde el año 2008)**[1] así como la optimización de recursos e incremento de la productividad de sus empleados obliga a la industria a transformar su metodología de trabajo convirtiendo a sus gestores en oficinas móviles.

La aceptación y firma de acuerdos y contratos entre la entidad financiera y el cliente a través de documentos físicos era uno de los obstáculos que entorpecía la agilidad en la gestión de documentos que las entidades financieras estaban buscando para dar un mejor servicio a sus clientes y reducir el coste de la oportunidad comercial.

Los procesos de contratación generan un grandísimo volumen de documentación el cual ha de ser enviado, firmado y archivado originando pérdida de tiempo y utilización de espacio físico.

Por otro lado, las tecnologías móviles ofrecen la posibilidad de optimizar los mismos procesos que actualmente se hacen en la oficina de la entidad bancaria y ahora pueden ser realizados en cualquier lugar y en cualquier momento.

Para ello es necesario estar soportado por una solución tecnológica sólida y segura, que permita agilidad, movilidad y ahorro de costes.

¿Qué es la Firma Biométrica?

El término biometría se refiere a las tecnologías basadas en el reconocimiento de unas características físicas unívocas e intransferibles de las personas para fines de autenticación e identificación.

Las características básicas que un sistema de reconocimiento biométrico debe cumplir son:

1. **Desempeño:** se refiere a la exactitud, la rapidez y la robustez alcanzada en la identificación de individuos por parte del sistema biométrico.
2. **Aceptabilidad:** indica el grado en que la gente está dispuesta a aceptar un sistema biométrico en su vida diaria.
3. **Fiabilidad:** refleja cuán difícil es desafiar al sistema.

La Firma Biométrica es la tecnología que permite capturar y asociar unívocamente la biometría del patrón grafológico de cualquier firma manuscrita, utilizando dispositivos especialmente diseñados para este fin, tales como Pads, Tabletas Digitalizadoras y Lápices activos.

Estos dispositivos, unidos a mecanismos de generación de firmas electrónicas, además de capturar la propia imagen de la firma (grafo), son capaces de reconocer y capturar el patrón biométrico de la misma, el cual es específico individualmente de cada ser humano.

Estos rasgos biométricos tienen en cuenta principalmente la velocidad y la aceleración de la escritura, la presión que se ejerce sobre la superficie al firmar, los cambios de dirección y el vuelo del lápiz. Todo ello dota de **mayor seguridad** a la firma realizada a través de este método.

Firma Biométrica vs Firma Digital
Dos soluciones de firma complementarias.

La **Firma Digital** es un tipo de firma electrónica que bajo un mecanismo criptográfico o un largo código numérico asignado a una persona da aceptación y autenticidad a un documento electrónico.

La firma digital normalmente reside en un ordenador o en algunos casos en un terminal telefónico móvil (tarjeta SIM) o en una tarjeta con chip criptográfico (tipo eDNI). Hay que considerar que las firmas digitales son tan seguras como el medio en el que residen (teléfono, tarjeta, etc.), el cual puede ser sustraído, extraviado, deteriorado, etc. Por lo tanto, el uso de una firma digital no siempre garantiza la identidad del emisor.

La **Firma Biométrica**, además del grafo y la imagen de la propia firma, permite capturar, establecer y reconocer comparativamente el **patrón biométrico** del grafo del firmante, como se detalla anteriormente. Estos rasgos son exclusivos de cada persona.

En el marco de la **Firma Biométrica**, además de la imagen de la firma en su aspecto gráfico, se incluye **información grafométrica** obtenida en tiempo real de un dispositivo especialmente diseñado para este fin y asociado al sistema de firma, vinculando esta información con el documento y el firmante de forma indisoluble. Además, se cifra dicha información de forma que no pueda quedar a disposición de nadie para su manipulación.

La firma biométrica representa un puente ideal entre la convención reconocida de la firma de un documento y la necesidad de documentos electrónicos para ser reconocidos únicamente por los individuos. Esta aplicación proporciona a los intervinientes la máxima seguridad y el control sobre los documentos creados digitalmente desde el origen, negociados y almacenados en el dominio digital.

Tecnologías Biométricas Combinadas

El uso de la biometría garantiza la autenticidad de la persona cuando interactúa con algún dispositivo de captura: lector de huella dactilar, lector de iris, registro de tecleo, registro de firma, etc., ya que se trata de características intrínsecas de cada persona.

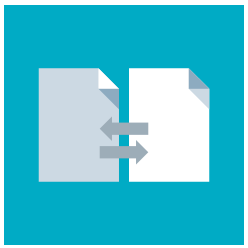
Sin embargo, debido a los cambios en los escenarios de captura (tipo de dispositivo, lugar en que se encuentra, luz de ambiente, ruido, etc.), se producen distorsiones en los datos capturados que generan falsos negativos que pueden provocar malestar en el usuario y desconfianza en el proveedor del servicio.

Para evitarlo, se propone el uso de dos o más factores biométricos capturados para el mismo acto de autenticación/identificación. Con el uso de dos o más factores biométricos se mejora significativamente la fiabilidad de la autenticación biométrica.

Actualmente, las tecnologías basadas en biometría están disponibles en los dispositivos de uso común de clientes y usuarios, como son Smartphone, ordenadores portátiles y las tabletas.

La ventaja del uso de las tecnologías biométricas combinadas es que aporta **autenticación fuerte**, necesaria cuando se trata de firma remota desatendida.

Retos de la Industria Finanaciera



Uno de los retos a los que se enfrenta actualmente el mercado financiero es el impulso de la **banca digital**, el uso de las nuevas generaciones de consumidores hacia modelos digitales, la **optimización de procesos** en la aceptación de documentación en formato electrónico de origen por parte de los clientes y procesos con documentación que necesita ser autenticada por el usuario.

Estos procesos generan la manipulación de un gran volumen de documentación que ha de ser firmada, enviada y archivada por parte de las entidades.

Tiempo, seguridad, espacio físico y un mejor servicio a los clientes hacen de estos procesos un área muy sensible para ser optimizada transformando la forma de trabajar de las empresas.

Gran parte de las entidades financieras buscan tecnologías más rápidas y fiables que proporcionen mayor eficacia y productividad a sus negocios acordes con las exigencias del mercado y las necesidades de sus clientes.

De la misma forma, el control de costes en la gestión de documentos físicos y el ahorro de tiempo a la hora de gestionar dichos documentos entre la entidad financiera y sus clientes, vienen a ser otros de los grandes retos a los se están enfrentando hoy y de cara al futuro.

Por otro lado, sus clientes, amparados en la normativa de protección de datos, exigen una mayor seguridad en el control de la gestión de riesgos, tanto en documentos físicos como virtuales.

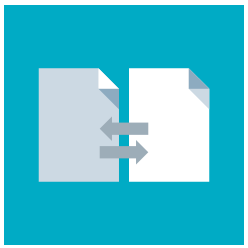
Casos de Uso.
La Firma Biométrica es un excelente sistema de identificación de la persona, que se aplica en muchos procesos debido a dos razones fundamentales: la **seguridad y la comodidad**.

La solución de Firma Biométrica sobre dispositivos móviles se ha convertido en pieza clave en la gestión de documentos entre entidad financiera y sus clientes, proporcionando ahorro en costes de papel, logística, espacio, tiempo y ofreciendo un altísimo grado de seguridad hasta ahora inalcanzables. Si a ello añadimos la **movilidad**, fomenta la proactividad y reduce el coste de oportunidad comercial evitando desplazamientos por parte de los clientes.

Aproximadamente el **90%** de las entidades financieras ya cuentan con una solución de firma biométrica fija, pero sólo el **20%** cuenta con la misma solución sobre dispositivos móviles.[2]

En el caso de las compañías aseguradoras el **10%** dispone de alguna solución de firma biométrica sin alcanzar el **1%** de las que disponen de una solución sobre dispositivos móviles.[3]

Características como singularidad, permanencia, universalidad, aceptabilidad y desempeño, hacen de la Firma Biométrica una tecnología con una enorme lista de áreas de aplicación en el sector financiero y compañías de seguros:



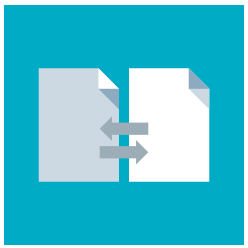
- **Firma de créditos hipotecarios**: donde la firma del cliente es imprescindible tanto en el contrato del propio crédito como en los seguros asociados: Vida, Hogar, etc.
- **Créditos Personales**: al igual que en los créditos hipotecarios la firma es obligada en el contrato y en el seguro asociado.
- **Apertura de cuentas**: donde la firma Biométrica sustituye a las antiguas fichas en las que quedaba registrada la firma y quedaba limitada exclusivamente a la oficina bancaria.
- **Solicitud de tarjetas de crédito**: donde la firma es obligada tanto en la solicitud como en la retirada de la tarjeta.
- **Retirada de dinero en efectivo**: en la ventanilla bancaria sustituyendo al recibo en papel al retirar o ingresar el dinero.
- **Firma de pólizas de seguro**: el cliente firma el contrato sobre el dispositivo móvil delante del agente evitando el desplazamiento del cliente a la oficina aseguradora y el envío de contratos en formato de papel.
- **Aceptación de trabajos realizados por siniestros**: donde el operario, una vez terminados los trabajos, requiere la firma del cliente sobre la orden de trabajo.
- **Cancelaciones de Pólizas**: ordenes de cancelación de pólizas evitando desplazamientos por parte de los clientes o el envío de la orden de cancelación.
- **Pago con tarjetas de cobertura médica**: como aceptación de factura que posteriormente será cargada a la compañía de seguros.
- **Tasaciones**: principalmente en las tasaciones de siniestros, para evitar alegaciones posteriores de las dos partes.

Movilidad + Agilidad = Productividad.

La transformación hacia la movilidad que las empresas quieren implementar a menudo requería la utilización de diferentes dispositivos en función de cómo y dónde se realiza el trabajo. En la actualidad con los dispositivos móviles basados en procesadores Intel han sido diseñados para satisfacer las necesidades de movilidad de sus usuarios y los requisitos de seguridad de las empresas.

Los dispositivos con tecnología de **pantalla táctil** han revolucionado la forma en que interactuamos con la tecnología, desde una pequeña tableta a un **AIO** (equipos todo en uno). Estos dispositivos permiten a los profesionales de una empresa estar reunidos alrededor de una sola pantalla en una interacción más natural.

Por otro lado, el empleado de oficina de hoy en día necesita el teclado tradicional y el ratón tanto para crear, presentar y colaborar. Los dispositivos 2 en 1 incorporan todo lo necesario en un dispositivo delgado, potente y fácil de llevar. Estos dispositivos (equipados con los procesadores proporcionan nuevos mecanismos de transporte y de uso para los trabajadores móviles en sus lugares de trabajo, con:



- **Diseños más ligeros**. Dispositivos más ultra-delgados que nunca, ya que no incorporan ventilador (una primicia para este tipo de dispositivo).
- **La máxima versatilidad en movimiento**, gracias a la fácil conversión de dispositivo con teclado en tableta de pantalla táctil, con un simple movimiento para ser desacoplado. La potente productividad del portátil, por lo tanto, está combinada con los activos ergonómicos de la tableta, proporcionando eficiencia y flexibilidad de acuerdo con las necesidades de cada momento.

El hecho de que el puesto de trabajo salga de la oficina permite a un gestor poder firmar la documentación necesaria tanto in-situ como en casa del cliente, y que este proceso de aceptación pueda eliminar el gran volumen generado de documentos en papel y optimizar la productividad de los gestores.

Uso de dispositivos móviles como nueva herramienta.

El uso de dispositivos móviles de última generación transforma de manera relevante el concepto de relación entre gestor y cliente.

Los dispositivos móviles ofrecen a las Entidades Financieras y a las Compañías de Seguros la posibilidad de transformar el enfoque de la oficina fija –donde el cliente ha de soportar colas y ser atendido en un puesto fijo– en oficina móvil, donde el cliente puede ser atendido en cualquier lugar de la oficina o en el propio despacho, y donde empleado y cliente interactúan de manera más personal sobre la misma información: el **terminal financiero**.

Tomando como ejemplo el "proceso de venta de una póliza de seguros", la compañía de seguros presenta al cliente el producto en sus diferentes modalidades (Teléfono, a través de publicidad o de un gestor que se desplaza a casa del cliente para explicar las características del producto).

Una vez el cliente se ha interesado por un determinado producto, la compañía de seguros hace llegar la documentación y el contrato al cliente (normalmente por correo) para que éste firme su conformidad en las diferentes copias: dos para la entidad y otra para el propio cliente. Las dos copias correspondientes a la entidad han de ser firmadas y enviadas de vuelta por correo.

Posteriormente, la documentación ha de ser revisada y archivada por la entidad aseguradora para su custodia.

Con la Solución de Firma Biométrica sobre dispositivos móviles, todos los pasos detallados en el ejemplo anterior habrían sido realizados entre el agente y el cliente en un solo paso, en cualquier lugar y en cualquier momento.

La percepción del cliente cambia significativamente al recibir un mejor servicio y al percibir en la entidad una mejor imagen de innovación tecnológica y modernidad.

La solución propuesta está compuesta por la aplicación de reconocimiento de firma biométrica ***"BeSign" (Serban Biometrics)****, combinada con los dispositivos móviles y la funcionalidad de seguridad y capacidad de gestión integrada de la tecnología Intel sobre Sistema Operativo* ***Windows* 8 de Microsoft*.***

Las características principales de la solución **BeSign** son:

- **La Multicanalidad**. Permite firmar un documento-e por varios medios legales de firma firmamediante certificado digital: e-DNI, tarjeta de claves bancaria, OTP´s, banca por internet (PIN+ OTP en el móvil), firma digital, etc.
- **BeSign** es aplicable a entornos tanto en fijo como en móvil y está soportado por diferentes plataformas: Java*, Linux*, Microsoft, iOS*, Android*.
- Además es **compatible** con entornos virtualizados Citrix*. Desarrollo único para canal de traspaso de datos entre servidor y clientes **ICA** (Arquitectura de Cómputo Independiente) de Citrix.
- Sistema de encriptación **AES 246 y RSA 2048**.
- Es **auditado bianualmente** por Auditores Jurídicos y Auditoría de Seguridad a nivel de código.

- **Cumplimiento normativo**:
  - **AES 246 y RSA 2048** (Seguridad).
  - **ISO32000-1** (Intercambio y visualización documentos longevos).
  - **ISO/IEC 19794-7** (Estándar de codificación y almacenamiento información biométrica).
- **Sellado y encriptación** de firma en cada documento firmado. Sin posibilidad de extraerla para uso y empleo en otros documentos. Cada firma va unívocamente asociada a un documento.

En el ámbito de las funcionalidades de la solución propuesta y con el fin de ofrecer el máximo de seguridad **"Serban Biometrics"** ofrece la posibilidad de la utilización de un conjunto de tecnologías biométricas combinadas denominada **"BeBiometrics"**.

Componentes de la solución

Los elementos necesarios para implementación de una solución de firma biométrica son:

- **Aplicación de reconocimiento de firma** biométrica, con capacidad de:
  - Registro de firma biométrica para alta de cliente.
  - Reconocimiento de patrones biométricos de grafo.
  - Discriminador de firmas.
  - Verificación de patrones biométricos.
  - Certificación de seguridad y jurídica.
  - Automatización de procesos.
- **Dispositivos móviles**, con capacidad de reconocimiento de firma biométrica y sistemas de seguridad integrados.
- **Sistema Operativo**, con sistemas de reconocimiento biométrico aprovechables por el desarrollo de aplicaciones a través de las API (Application Programming Interface) de marco Biométrico.

Definición de la Aplicación: Funcionalidades y procesos.

El proceso de reconocimiento de firma biométrica comienza con el **registro de datos del cliente** en los sistemas de la entidad financiera. Este proceso se produce una sola vez cuando el cliente se da de alta en la entidad financiera. Además de los datos generales, el cliente deja registrada su firma sobre un dispositivo con capacidad de reconocimiento de firma biométrica. Todos estos datos quedan registrados en la base de datos centralizada de la entidad. Cuando un documento ha de ser firmado por un cliente el proceso se compone de las siguientes fases:

1. **Solicitud del documento**: desde el dispositivo móvil, se solicita el documento a ser firmado que se obtendrá en formato PDF con un Hash asociado (algoritmo que produce un valor alfanumérico de longitud normalmente fija que representa un resumen de toda la información que se le ha dado). En él se especifica la información que va contenida, de forma que cualquier usuario que lo recibe puede interpretar todos los detalles: quién lo debe firmar, en qué orden y dónde se van a situar las firmas (coordenadas). El documento se visualiza en el dispositivo a través de un archivo XML (archivo electrónico estándar para intercambio de información). El documento nunca reside en el dispositivo móvil, siempre reside en el servidor.

2. **El documento es enviado al sistema de firmas**: en este proceso aparece un cuadro de espacio reservado para la firma. Durante este paso, si se modificase un solo bit del documento original también cambiaría el hash.

3. **Captura del Patrón Biométrico**: cuando los intervinientes proceden a la firma del documento, el dispositivo móvil es capaz de reconocer la presión, aceleración, velocidad, movimientos vertical y horizontal que se ejercen sobre la pantalla e incluso el vuelo del lápiz cuando la firma consta de trazos discontinuos.

4. **Timestamp** (sello de tiempo): la firma queda vinculada con el documento en el momento en que este ha sido firmado. El **Timestamp** es un mecanismo en línea el cual permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo, por lo que las firmas quedan vinculadas con el documento en el momento en que este ha sido firmado. Mediante la verificación en tiempo real de la firma (**inclusión de sellado en el tiempo**) y la **geo-localización**, se consigue un mayor control sobre el firmante, evitando así intentos de fraude, de suplantación de identidad o de repudio o negación de un documento ya firmado; al tiempo que permite controlar los procesos de firma y guardar el rastro y la traza de las firmas realizadas. El timestamping puede ser dado por el servidor de la aplicación o puede ser insertado un Timestamping de un tercero de confianza, dándole más valor al documento.

5. **Toda la información y composición del documento se realiza en el servidor y queda contenida en un documento PDF/A como Metadata.** Los elementos

de dicho documento PDF/A son: los contenidos, anexos cifrados, firmas con sus características, etc.) Todo ello es cifrado a través de una clave pública que se facilita en el momento de enviar la información.

6. **El documento PDF/A es sellado con un certificado digital de la entidad**, lo que prueba la **integridad** del documento. La firma biométrica imposibilita cualquier tipo de manipulación del documento firmado, garantizando de esta forma la autenticidad de las firmas de las personas y entidades que intervienen en el intercambio de información además de la **confidencialidad de los datos**, ya que sólo el emisor y el receptor pueden ver la información contenida. La firma del documento puede ser interna, es decir, con un certificado de empresa o autogenerado por la propia entidad; o para dar más valor y añadirle aun más seguridad al documento esta firma puede ser realizada por un tercero de confianza.

El documento y las claves quedan avalados y custodiados por un **tercero de confianza** (entidad independiente que avala la autenticidad de la firma), el cual es custodio de las claves de cifrado y sellado de los documentos. En función del **riesgo** de la operación (determinado por la entidad financiera), el tercero de confianza inserta un Timestamping para dotar de mayor garantía al documento firmado.

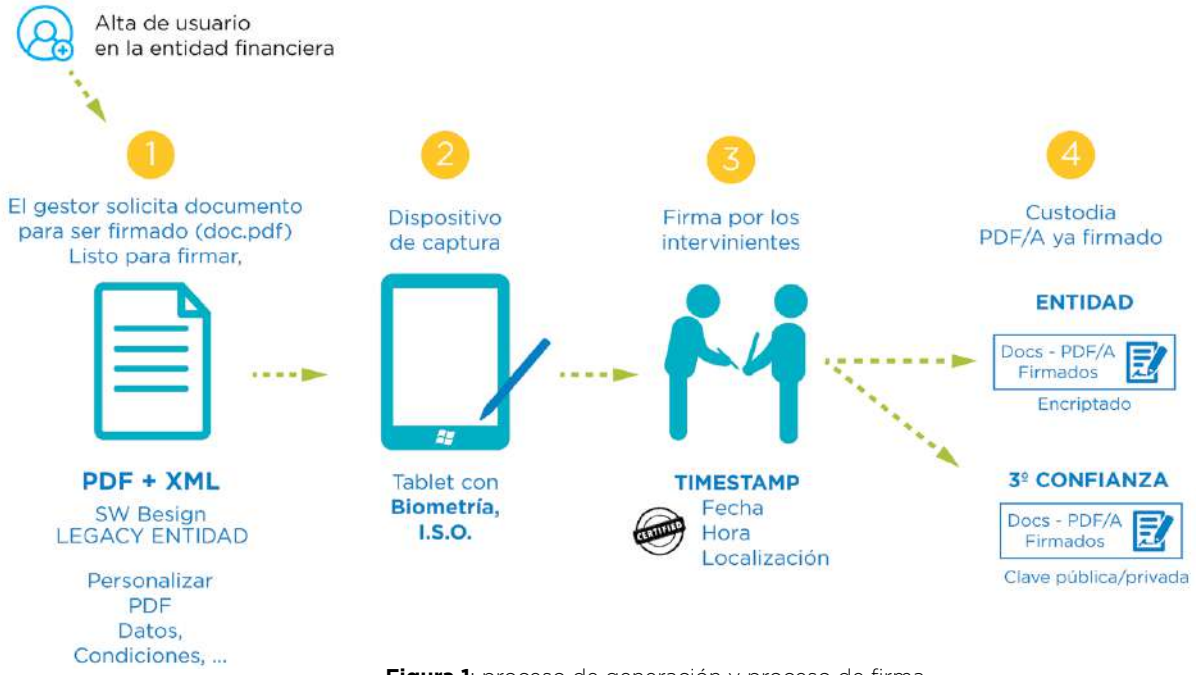


Figura 1: proceso de generación y proceso de firma.

Proceso de verificación (en caso de repudio)
En caso de ser necesaria una **verificación por rechazo o repudio por parte de alguno de los intervinientes**, el sistema comparará la firma recogida en el documento con aquellas firmas indubitadas que se recogerán en el momento del litigio. **El tercero de confianza** es el único poseedor de las claves para el descifrado del documento, con lo que esta entidad toma una especial relevancia en el proceso de **verificación**.

El **Tercero de Confianza**, también denominado **Mediador de Confianza**, es una entidad homologada y neutra que actúa de "**Notario Digital**".

Una vez desencriptado el documento, es un proceso simple, al tener que contrastar únicamente dos muestras, en el que el resultado puede ser positivo o negativo.

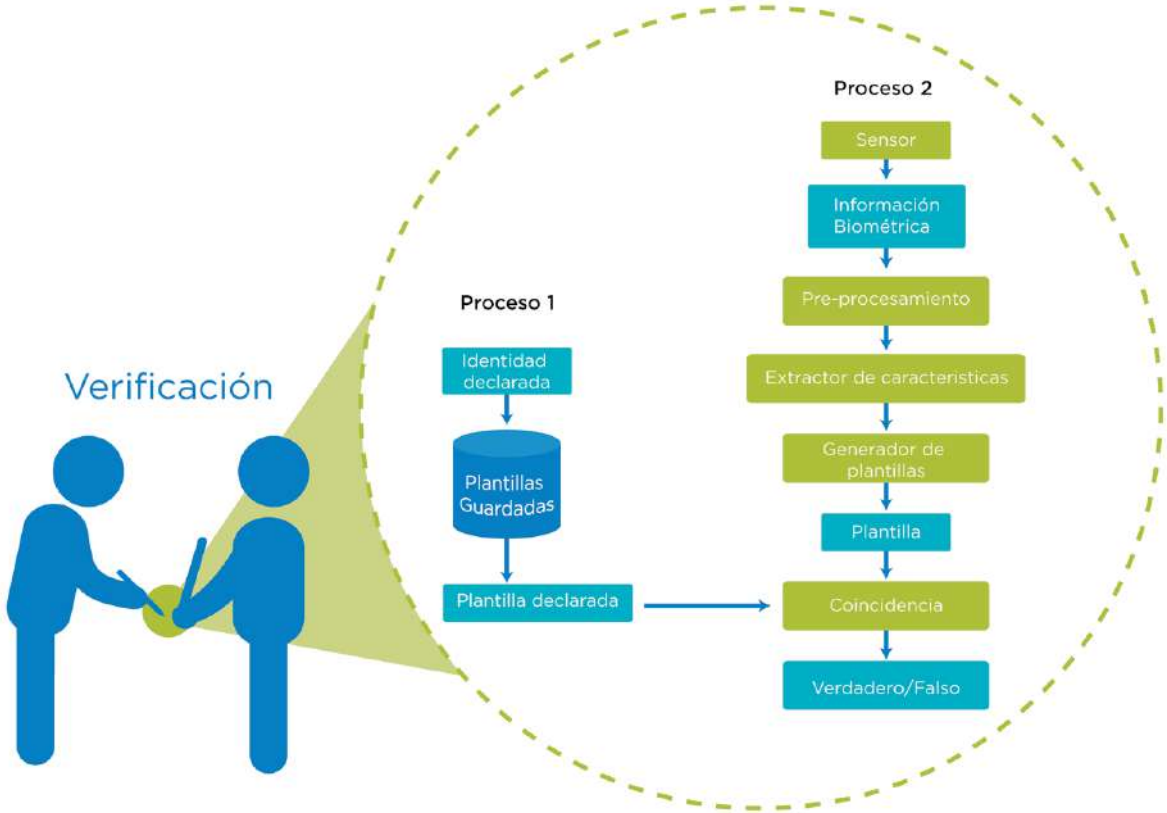


Figura 2: proceso de verificación de firma (en caso de repudio).

Descripción de dispositivos: Dispositivos Móviles, Capacidades de captura de firma biométrica.
Los dispositivos necesarios para la Firma Biométrica son: Tabletas digitalizadoras conectadas a ordenadores personales y tabletas generalistas preferentemente capaces de registrar el trazado de la firma escrita y todos sus aspectos y dotadas con tecnología sensible a la presión del puntero de firma.

Dentro de los dispositivo móviles homologados para la solución de firma biométrica destacan los dispositivos detachables (2 en 1) HP Elite X2 1011 y las tabletas HP Elite Pad 1000 con tecnologías de procesador Intel Core M e Intel Atom Z2795 respectivamente.

Por sus características y prestaciones estos dos dispositivos se han convertido en la solución idónea tanto para trabajar en la oficina como para trabajar en entorno móvil. Cabe destacar su versatilidad, fácil manejo y ligereza. Un ordenador portátil y una tableta integrados en un solo dispositivo. Únicamente deslizando la pantalla se pasa de un portátil a una Tablet.

Dependiendo de la tecnología de captura biométrica que posea cada uno de los dispositivos móviles es necesario el uso del lápiz, el cual es capaz de detectar la presión, velocidad y vuelo que ejercemos a la hora de firmar.

Solución Multicanal - Formas y Métodos de Firma a través de diferentes dispositivos y canales
La solución de firma biométrica **BeSign es multicanal** y acepta diversos tipos de identificación y firma con integración completa del documento firmado a través de los diferentes productos e independiente de los dispositivos y medios empleados en la ejecución de firmas diferidas o multi-firmas.

BeSign está adaptada a diferentes arquitecturas, sistemas y canales permitiendo la firma de un mismo documento con otros canales de firma, utilizados en la mayoría de escenarios donde un reconocimiento de firma e identificación es requerido:

- Entornos donde la firma es requerida a través de un dispositivo con capacidad de reconocimiento de **firma biométrica**.
- Donde la identificación y firma a través de un teclado, se solicita con **tarjeta de coordenadas**.
- En gestiones donde es necesario el uso de un **certificado digital** (Firma Digital).
- En casos de identificación que requiere un **código o** donde la identificación y firma a través de un teclado, se solicita con **tarjeta de coordenadas**.
- DNI electrónico.

Figura 3: diferentes canales de identificación aceptados por BeSingn.

Validez Jurídica y legal. Autenticidad de Firmas e integridad de documentos.

La firma biométrica como elemento de identificación cumple con los tres requisitos que se plantean como exigencia desde un punto de vista legal: **Autentificación, Integridad** y **No Repudio**. Esto es autenticar y acreditar fehacientemente al autor de la firma, probar la integridad de los datos biométricos asociados al documento y del propio documento firmado y dar **validez jurídica** por la vinculación biunívoca a cada persona que firma.
No existe una normativa específica con respecto a la validez de la Firma Biométrica, pero desde un punto de vista jurídico, un sistema de firma electrónica avanzada, utilizando soluciones de tecnologías biométricas, puede ser utilizado para crear firmas digitales que tienen la misma capacidad jurídica de la firma manuscrita en papel de conformidad con el **artículo 5.1** de la Directiva Europea de Firma Electrónica. Esto es debido a que "ambos se regirán por las reglas generales de la **Prueba**".

Actualmente la normalización de los procesos de certificación jurídica se encuentran bajo los **"Dictámenes de la Superintendencia de Banca y Seguros" (SBS)**. Dichos dictámenes son revisados cada dos años en función de la evolución de la tecnología.

Por otro lado, la Firma Biométrica es compatible complementariamente con la nueva legislación sobre firma electrónica como puede comprobarse en el último borrador del Reglamento Europeo – "Identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior".

De acuerdo con recientes publicaciones, la seguridad jurídica de la firma avanzada debe pilotar sobre **10 principios básicos**:

1. Captura de elementos biométricos dinámicos de la firma asociados a sus datos de producción.
2. Vinculación biunívoca de los elementos biométricos con el documento firmado.
3. Imposibilidad de incrustar la firma en otros documentos.
4. Integridad de los datos firmados.
5. Autenticidad del documento y vinculación con el firmante.
6. Confidencialidad de los datos biométricos y Protección de la información conforme a la LOPD.
7. Posibilidad de comprobar biométricamente la firma por el titular.
8. Posibilidad de demostrar la validez y vinculación biunívoca de la firma en un proceso litigioso.
9. Simetría probatoria.
10. Soporte duradero.

La solución **BeSign de firma biométrica** cumple con todos los requisitos de la definición de Firma Electrónica en la Directiva Europea.

Figura 4: certificación jurídica y legal.

Normativa relevante e hitos sobre firma biométrica

Datos de interés:

- **Diez millones de clientes** utilizaron alguna solución de firma biométrica durante el año 2.012.
- Durante el año 2.012 se ejecutaron **200 millones** de operaciones.
- En el año 2.014 la cifra ascendió a **850 millones** de operaciones.
- De estos 850 millones de operaciones sólo se procedió a la revisión de **37 casos** por repudio y sólo uno llego a juicio.

En el mercado están disponibles algunas soluciones de reconocimiento de firma que ofrecen diferentes prestaciones. Sin embargo, para asegurarnos de implementar la solución más completa, inteligente y segura, deberemos de tener en cuenta una serie de consideraciones:

Aplicación: la aplicación debe cubrir todas las expectativas y necesidades de los clientes. La automatización de los procesos, los sistemas de seguridad, parámetros de reconocimiento de firma, el diseño para trabajar en un entorno Web o de virtualización y la integración con los sistemas corporativos toman especial relevancia para el éxito de la solución. La estabilidad del aplicativo así como el mantenimiento del mismo ofrecen una mayor seguridad al responsable del departamento de TI.

El correcto funcionamiento y la capacidad de un sistema de reconocimiento de Firma Biométrica se puede valorar por medio de una serie de **tasas de trazabilidad**.

Sistema Operativo: las empresas son contrarias a correr riesgos cuando hablamos de plataformas de Sistemas Operativos. Buscan un Sistema Operativo robusto, ágil, con una implantación empresarial generalizada, que les asegure un ciclo de vida duradero y que posea una gran capacidad de integración con la base actualmente instalada.

Aunque muchas organizaciones, la hora de definir su estrategia de movilidad también están considerando plataformas móviles alternativas, como iOS o Android, los usuarios de Windows siguen muy comprometidos

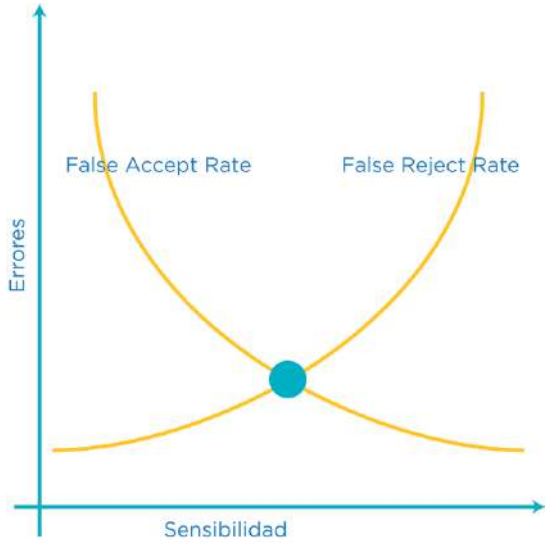


Figura 5: índices de efectividad de un sistema biométrico de identificación y verificación.

con sus plataformas. Capacidades como la estabilidad de la plataforma y la seguridad, integración con los sistemas corporativos, la infraestructura de gestión y el apoyo continuo a las aplicaciones existentes, son factores que conducen a la utilización del sistema operativo Windows para las soluciones móviles más relevantes del mercado. El uso de soluciones de Windows para aplicaciones móviles de primera línea está generalizado y representa la plataforma común para la mayoría aplicaciones empresariales importantes.

Las empresas ven una oportunidad en la utilización de dispositivos móviles, ya que cualquier operación en la que fuera necesaria la participación del cliente para la aceptación o firma de documentos, ahora se puede hacer desde cualquier lugar, en cualquier momento y sobre un dispositivo ligero y robusto. Para ello, las empresas buscan dispositivos móviles que aporten robustez, seguridad, fiabilidad y estabilidad, autonomía y con largo ciclo de vida.

Los dispositivos móviles son una herramienta tremendamente poderosa para la optimización de los negocios. La inmensa mayoría de los más altos ejecutivos de las compañías opinan que la movilidad afectará positivamente a sus negocios.

La elección del dispositivo móvil idóneo es clave para la implementación de la solución de firma biométrica. Para que la elección tenga éxito existen algunas consideraciones a tener en cuenta:

- El dispositivo móvil debe estar equipo con tecnología de última generación. Altas prestaciones con un mínimo consumo con el fin de llevar la movilidad al máximo nivel.
- Los departamentos financieros buscan un rápido **retorno de la inversión**. Los dispositivos móviles deben asegurar un alto rendimiento, un largo ciclo de vida y no tener un alto coste de mantenimiento, además de incrementar notablemente la productividad de los empleados.
- Reducir el número de accesorios adicionales alrededor del dispositivo móvil. El dispositivo debe incluir todo lo necesario para realizar correctamente las tareas de los gestores.
- También es muy importante que los dispositivos se integren perfectamente en el entono de TI ya existente en la compañía.
- El dispositivo móvil elegido no sólo debe disponer de pantalla táctil, sino que además debe poseer capacidad para capturar y almacenar factores biométricos, como la velocidad, la presión o el tiempo que el lápiz se encuentra en el aire entre trazo y trazo.

Los dispositivos móviles pueden incorporar diferentes tipos de tecnología de captura de firma biométrica:

- **EMR** (Wacom*): Tecnología de resonancia magnética. Combina sensores finos, algoritmos sofisticados y transmisiones de datos ultrarrápidas. La Tecnología Wacom consta de tres capas: Una para la detección de los dedos, otra la pantalla LCD y una tercera capa de detección EMR **(Resonancia Magnética)**, que detecta la emisión electromagnética del lápiz. Al ser una tecnología basada en la pantalla del dispositivo no va alimentada con baterías.
- **Ntrig Active Pen**: Tecnología de lápiz activo. La Tecnología Ntrig cuenta con dos capas: La primera de detección de dedos y lápiz activo y una segunda capa LCD. Incorpora botones configurables y puntas de lápiz intercambiables. Se alimenta con batería que debe ser cambiada una vez se haya agotado.

- **Synaptics*** Active Pen: Tecnología de lápiz activo que realiza la comunicación con la tableta a través de la tecnología Bluetooth*. Incorpora una serie de botones que permiten aprovechar al máximo las prestaciones del sistema operativo Windows 8. El lápiz incorpora una batería que debe ser remplazada cuando se agota.

- **Atmel* MaxStilus*** Active Pen: Tecnología de lápiz activo. Incorpora un sensor que detecta 256 niveles de presión y tecnología de rechazo de la palma de la mano para evitar incorporación de datos erróneos en la pantalla. Se alimenta con batería.

Con los dispositivos móviles equipados con los procesadores Intel Core M e Intel Atom Z3000 todas las consideraciones y necesidades anteriormente descritas quedan totalmente cubiertas.

Arquitectura Intel®

Diseñado específicamente para las últimas tabletas con Windows 8.1, el procesador Intel Atom serie Z3700 ofrece un excelente rendimiento con cuatro núcleos de procesamiento y gráficos **Intel® HD** con tecnología **Intel® Clear Video HD**. La eficiencia energética con diseño **system-on-chip (SoC)** ayuda a conservar la energía de la batería y permite diseños delgados y ligeros.

La tableta incorpora el procesador **Z3795**, certificado para la versión Windows 8.1 de 64 bits. Además de aumentos de rendimiento y mejor experiencia de usuario con los dispositivos, el soporte de 64 bits evita, a aquellas organizaciones que hayan completado la migración al entorno de 64 bits en su totalidad, el empleo de las mismas versiones de aplicaciones en el entorno de **HP1000** que en el resto de dispositivos y reduce la complejidad y número de imágenes en la gestión de imágenes de sistema operativo en el entorno Windows.

Los procesadores **Intel® Core M** ofrecen un rendimiento significativamente muy mejorado, incluyendo Gráficos y la duración de la batería, en diseños delgados y ligeros. Las nuevas mejoras incluyen:

- Un diseño eficiente de la energía en combinación con la tecnología de fabricación de 14nm permite una reducción del 60% en el punto térmico de diseño (TDP), para factores de diseño más delgados, silenciosos y sin necesidad de la incorporación del ventilador.

- Un nuevo paquete multichip que tiene un tamaño casi un 50% más pequeño que los procesadores de cuarta generación **Intel® Core ™ (serie Y),** lo que permite diseños de plataformas más pequeñas.

- El nuevo procesador de bajo consumo ofrece un rendimiento más rápido y un mejor rendimiento de gráficos en comparación con las generaciones anteriores.

Los nuevos dispositivos móviles 2 en 1 ofrecen todo en un solo paquete: un ordenador portátil multipropósito y una tableta.
Están diseñados para profesionales que demandan un alto rendimiento de sus dispositivos y para todo tipo de usos: tanto consulta como creación de contenidos, pudiendo sustituir al ordenador desktop.

La tecnología incorporada en los dispositivos **HP Elite X2 1011**, supone una innovación de importancia considerable en la transición hacia un entorno sin cables y expande el concepto de dispositivo para movilidad al de área de productividad personal.

Finalmente los procesadores incorporan la tecnología que permite habilitar soluciones de autenticación fuerte (Second Factor Authentication), gestión de certificados digitales y protección de transacciones basadas en hardware.

El robo de identidad es una creciente preocupación global para personas y empresas. Se requieren soluciones seguras pero fáciles de usar ya que los hackers inventan nuevos métodos para obtener los nombres de usuario y contraseñas.

Con la tecnología habilitada en dispositivos 2 en 1 y en las tabletas, se ofrece un hardware de confianza que puede ser utilizado por las soluciones de autenticación de múltiples factores. Los sistemas de hoy en día ofrecen métodos adicionales de protección de identidad y verificación de transacciones que pueden ayudar a la organización a implementar soluciones robustas de autenticación fuerte y soluciones de protección de identidad.

Además, se utiliza un **One-Time Password (OTP)**, uso exclusivo de una sola vez de un número de seis dígitos que se genera cada 30 segundos desde un chipset integrado, a prueba de falsificaciones, el cual permite la autenticación de dos factores seguros y sin problemas de acceso a VPN. Todo esto sirve para confirmar la presencia del usuario, verificar las transacciones, y proteger la pantalla de un PC del acceso de un malware mediante la creación primero de una entrada de PIN seguro antes de la liberación de credenciales y la creación de una ventana que no puede ser vista por un hacker.

Con **Intel IPT/NFC**, los usuarios pueden conectarse a un Intel IPT con un comercio o página de pago dotado con **NFC**, pagar por un producto pulsando en su tarjeta de crédito dotada con **NFC** sobre un sensor **NFC** conectado en el equipo y completar la transacción con autenticación positiva de identidad por Intel IPT.

La tecnología **Intel IPT** con **PKI** utiliza el motor de administración de Intel para proporcionar una solución de seguridad basada en un hardware similar a la de otros módulos de seguridad de hardware, como las tarjetas inteligentes.

A diferencia de la mayoría de los módulos de seguridad de hardware, **Intel IPT-PKI** está diseñado para ser manejado como software, pero el hardware es resistente a la manipulación. La seguridad basada en hardware se logra mediante el uso del Intel® Management Engine **(Intel® ME)** para realizar todas las

operaciones criptográficas. De esta manera, las teclas no están expuestas al software que se ejecuta en la unidad central de procesamiento de la computadora **(CPU)**. Por otra parte, todos los certificados están ligados a la plataforma en la que se crean.

HP - Rendimiento, Gestión y Seguridad

Los bancos y las compañías de seguros se sienten atraídas por empresas que cubran sus necesidades de manera consistente.

Para **profesionales móviles** que se encuentran en constantemente movimiento es muy importante que la tecnología soporte golpes y caídas y esté disponible en todo momento con una gran autonomía. Necesitan una conectividad rápida y un rendimiento fiable para asegurar que el trabajo se realice apropiadamente

Lo que necesita: movilidad, durabilidad, conectividad.

Para los **altos ejecutivos** de las compañías, una oficina de "c-suite" necesita un PC "c-suite", diseñado para el estilo de clase ejecutiva y el rendimiento. Con la sobrecarga de trabajo necesitan tener acceso a sus datos de forma rápida. Manejan información confidencial y tienen la necesidad de asegurarse que toda esta información permanece segura.

Lo que necesita: seguridad, rendimiento y fiabilidad.

Figura 6: capacidades de seguridad y gestión de los procesadores.

El **HP Elite Pad 1000 G2** está diseñado para los profesionales que necesitan movilidad y maximiza la productividad con la comodidad de una tableta. Esta tableta emplea un procesador Intel Atom de cuatro núcleos, 4GB de memoria y 64 o 128GB de almacenamiento y es, por tanto, capaz de trabajar perfectamente con Windows 8 y rendir al máximo con una duración de batería extraordinaria.

Esta serie de características lo hacen muy interesante para entornos profesionales, pero donde marca definitivamente la diferencia es en la gama de accesorios para adaptarlo a distintos entornos. Existen adaptadores **"Jackets" (Chaquetas)** que envuelven la tableta, la protegen y amplían sus conexiones y su protección frente a caídas. Están disponibles varios modelos:

- **Security Smart Jacket**, incluye lector de SmartCard y de huella dactilar para autenticar al usuario.
- **Productivity Smart Jacket**, con teclado Bluetooth.
- Y por último, una dirigida al sector **hospitalario y de salud** y otra que convierte a la tableta en un **punto de venta**.

Adicionalmente existe la posibilidad de añadir un **Stylus Atmel** que detecta 256 niveles de presión y que, con el software adecuado, permite reconocimiento de firma biométrica.

Figura 7: Tablet HP ElitePad 1000 G2 con Productivity Smart Jacket.

Tecnologías Complementarias para las Soluciones de Firma Biométrica.

Se conocen actualmente entre 20 y 30 tecnologías biométricas implementables, cada una con sus propias características que las pueden hacer más adecuadas para una aplicación u otra. La combinación de dos o más tecnologías biométricas en una solución integrada está teniendo un rápido desarrollo tecnológico y despliegue comercial, al aportar mayor flexibilidad y precisión.

A continuación se detallan las principales características de las soluciones biométricas más comunes:

Huella dactilar: la identificación a través de huella dactilar está plenamente extendida siendo usada durante decenas de años. El dispositivo de captura puede ser un periférico de escritorio o un lector integrado en el dispositivo móvil.

Reconocimiento facial: este tipo de identificación se basa en la estructura facial del individuo, registrada por una cámara midiendo distancias y relaciones entre puntos y creando un modelo único de cada persona. Los dispositivos más usados son las cámaras de video o las cámaras integradas en el PC o tableta.

Reconocimiento de iris: a través del escaneo del iris una cámara registra una imagen del ojo del individuo recogiendo un modelo único. El “código iris” genera una de las huellas más precisas entre todas las tecnologías biométricas. El dispositivo utilizado para el reconocimiento de iris es una cámara de infrarrojos.

Reconocimiento de voz: el proceso de reconocimiento de voz depende de las características de la estructura física del tracto vocal de un individuo así como también de sus características de comportamiento. Este reconocimiento se realiza a través de un micrófono o teléfono.

Reconocimiento de la geometría de la mano: la verificación de la palma de la mano es sencilla, económica, segura y de gran aplicación en distintos ámbitos económicos. Se realiza con un escáner capaz de reconocer el patrón de las líneas de la palma de la mano.

Reconocimiento de escritura sobre teclado: la dinámica de tecleo es una rama de la biometría que se dedica al estudio del reconocimiento del patrón de tecleo de un usuario. Este patrón se basa en la velocidad y presión que un individuo ejerce al escribir sobre un teclado. El dispositivo utilizado es el propio teclado.

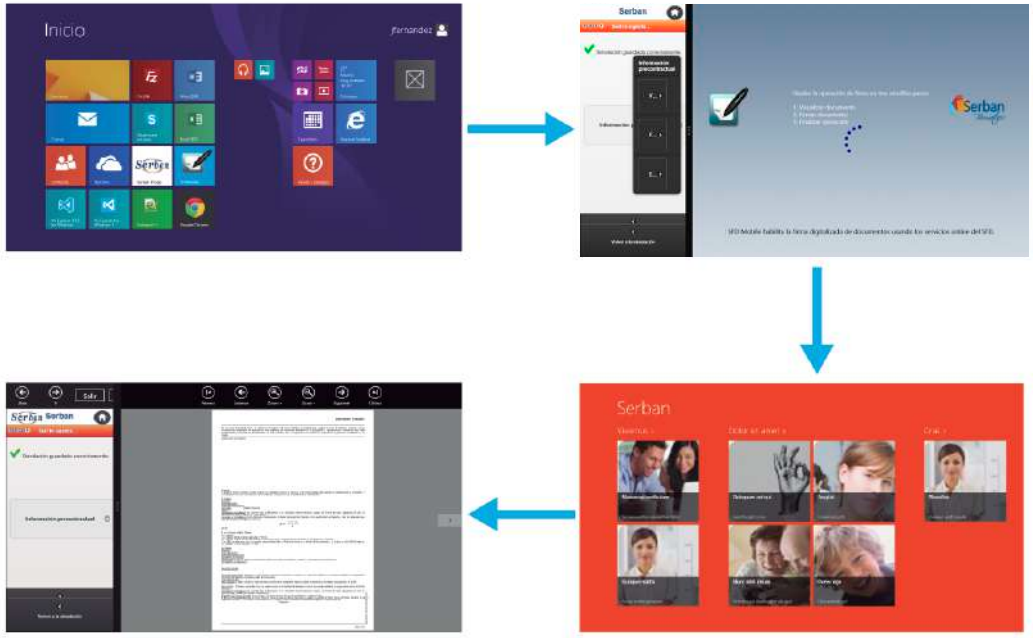
Y todas estas tecnologías combinadas se ven aún más reforzadas con la tecnología de protección de la identidad**.**

Percepción del Usuario ante la Solución.
Como la mayoría de las personas están acostumbradas a utilizar sus firmas durante interacciones con los clientes o proveedores, la Firma Biométrica se considera menos invasiva que otras técnicas biométricas.

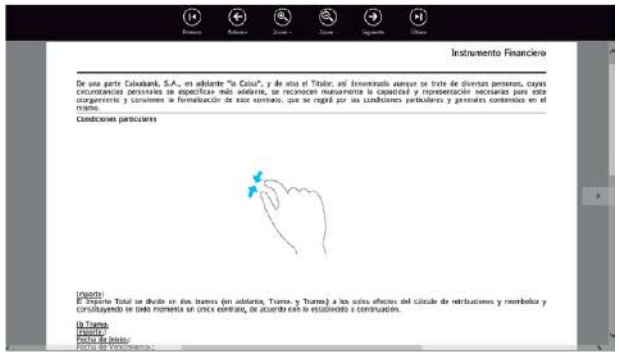
El documento no sale del servidor central donde se encuentra almacenado y es presentado en la pantalla del dispositivo móvil en formato PDF con el espacio preparado para ser firmado y por tanto, la sensación del cliente al proceder a la firma sobre el dispositivo móvil es la misma que la de firmar sobre papel, más teniendo en cuenta que la firma es archivada en tiempo real.

Tanto gestores como clientes pueden acceder de una manera fácil y rápida a la aplicación de firma biométrica **BeSign** desde la pantalla táctil del dispositivo móvil y a través de los iconos del sistema operativo Windows 8.1.

Una vez la aplicación está en funcionamiento, se presentan las opciones de **Visualizar documento, firmar documento y finalizar operación**.



Con el documento seleccionado en pantalla, el usuario tiene la posibilidad de hacer zoom utilizando los botones situados en la parte superior o bien deslizando dos dedos sobre la superficie de la pantalla del dispositivo. Esta herramienta es de gran utilidad para visualizar el documento con mayor facilidad.



Pulsando el botón **"Firmar"** situado en la parte inferior de la pantalla, el usuario puede ver una ventana con los nombres de los firmantes con la posibilidad de **firmar u omitir**.

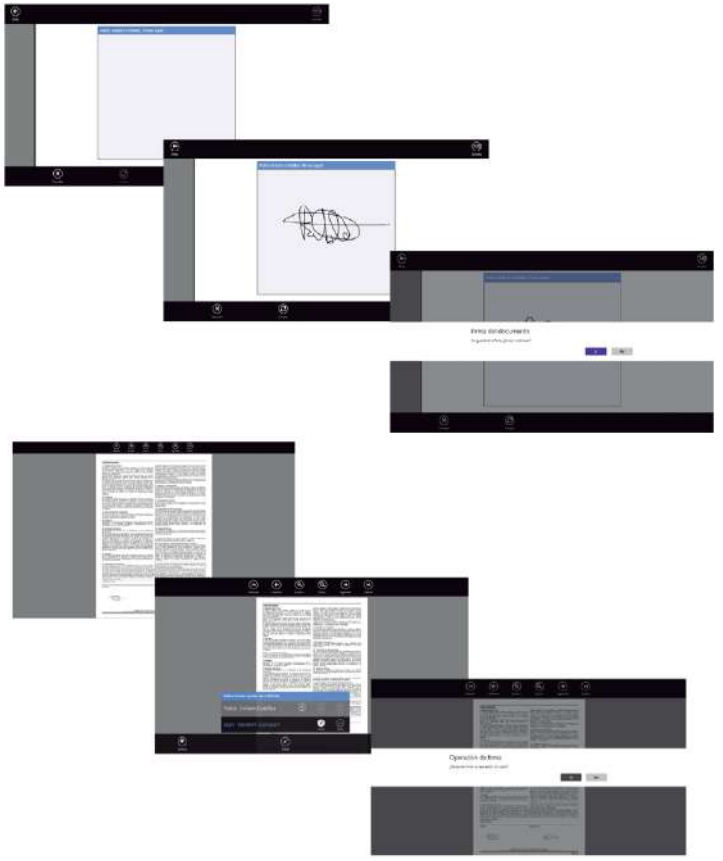


Figura 10: enviada la firma al servidor, el usuario puede explorar el documento firmado y pasar a la firma del siguiente firmante.

Cuando el usuario selecciona el firmante, el recuadro del área de firma se amplia para mayor comodidad. Una vez firmado se habilitan dos botones: **Aceptar**, inicia el envío de la firma asociada hacia el servidor de biometría. **Cancelar**, borra todos los trazos para poder proceder a una nueva firma. Aceptada la firma, se requiere una nueva **confirmación** para continuar con el proceso.

Consideraciones sobre el Diseño de la Plataforma. Tipologías de integración.

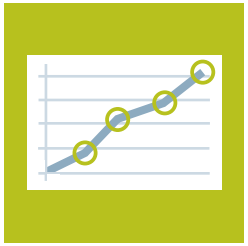
Tras un periodo de consultoría y análisis, en función de la plataforma tecnológica que actualmente posea la entidad, existen una serie de consideraciones a tener en cuenta cuando se procede a la toma de decisión de la implantación de una solución de Firma Biométrica:

- **Infraestructura desplegada actualmente en cliente**: es muy importante conocer y entender la infraestructura que el cliente posee en la actualidad para que la implantación del nuevo sistema esté correctamente dimensionado y se integre sin ningún problema de compatibilidad.
- **Estudio de volumetría**: en base al volumen de documentación que gestiona una compañía durante un periodo de tiempo determinado, es necesario realizar un análisis del mismo estableciendo así un dimensionamiento adecuado del alcance y la infraestructura de la solución.
- **Prueba de stress**: se establece una prueba de stress del sistema para la evaluación y dimensionamiento en función del número de tareas y dispositivos móviles accediendo concurrentemente al sistema.
- **Tipología de documentación**: en función de los diferentes tipos de documentos que se manejan en una entidad financiera, las plantillas deben ser adaptadas y sincronizadas para su correcto funcionamiento.
- **Estudio de utilización de sistema MDM (Mobile Device Management)**: con el fin de implementar un sistema de gestión centralizada de los dispositivos móviles que forman parte de la solución.
- **Entorno fijo o de movilidad**: en función del entorno de trabajo, la solución debe ser diseñada para trabajar en oficina, donde sólo se tendrá en cuenta la implementación de dispositivos fijos con el accesorio de captura de firma biométrica correspondiente o en entorno móvil, donde además de los dispositivos de la oficina la solución debe contar con tabletas capaces de reconocer firma biométrica.
- **Estudio de compatibilidad**: la solución de Firma de Biométrica **BeSign** de **Serban Biometrics** es compatible con cualquier tipo de dispositivo criptográfico que cumpla con los requerimientos de reconocimiento biométrico.

Por último, en una solución donde se están tratando datos biométricos de las personas, la seguridad se convierte en pieza clave de la solución. Las medidas de seguridad señaladas por la LOPD y su reglamento de desarrollo no solo se consideran exigencias para el cumplimiento legal, sino también buenas prácticas que mitigan y evitan posibles incidencias en relación a la privacidad de los usuarios.

Aplicabilidad a otros Sectores con retos similares
El Sector Financiero y Compañías Aseguradoras no son las únicas industrias susceptibles para la implantación y utilización de la tecnología de firma biométrica. Existen muchos otros sectores con retos similares en donde la seguridad en identificación de personas así como la optimización de recursos hacen de la solución propuesta un activo indispensable.

- **Sanidad**: el **consentimiento informado** es el documento que más papel genera en hospitales y centros de salud. Es una obligación legal y su conversión a un documento electrónico supone muchos beneficios en términos de eficiencia, reducción de costes y cumplimiento normativo. La autorización por parte de un paciente o del familiar más allegado para proceder a una intervención quirúrgica, la firma por parte del médico del alta de un cliente después de una hospitalización, la firma de la receta médica e incluso un acta de defunción son casos sensibles donde la aplicación de la solución de firma biométrica toma especial relevancia.
- **Administración Pública**: identificación de personas que viajan y han de ser visadas en las aduanas, entrada en edificios públicos e incluso reconocimiento de firmas en documentos públicos, solicitudes, certificación de documentos, etc.
- **Inmobiliarias**, además de todas aquellas empresas donde la firma de documentos sea parte indispensable de su proceso diario. En cualquier notificación notarial o legal, escrituras públicas, testamentos, cesiones, venta o alquiler de inmuebles, es necesaria la aceptación y firma de la documentación.
- **Comercio e Industria**: en los establecimientos, pagos en caja, servicio al cliente, firma de contratos, logística... En todos estos casos la firma es necesaria para la confirmación de recepción de material así como la aceptación del pago.
- **Judicial**: Expedientes electrónicos, procesos judiciales, denuncias, demandas, etc.
  En un juzgado existe un elevadísimo volumen de documentación para ser firmada tanto por letrados, secretarios y ciudadanos. Cesión de poderes, registro de notificaciones y demandas, sentencias y cualquier otra documentación que entra en un juzgado ha de ser firmada por y en el registro para que tenga validez.



La utilización de sistemas de reconocimiento basados en biometría sobre dispositivos móviles supone grandes beneficios para las organizaciones o entidades que los implantan. Al permitir la generación de documentos electrónicos en origen, se puede prescindir del formato físico, lo que permite conseguir ahorros de costes importantes gracias a la eliminación del papel, su manipulación, transporte, almacenamiento y archivo, entre otros, además de los tiempos dedicados a la búsqueda y gestión de los documentos firmados y archivados.

La solución propuesta que se describe en esta guía se centra en ayudar a las empresas del Sector Financiero y Compañías Aseguradoras a optimizar sus procesos en la firma de documentos sobre dispositivos que permiten una absoluta movilidad. Los beneficios clave que la solución propuesta puede ofrecer para los negocios, son:

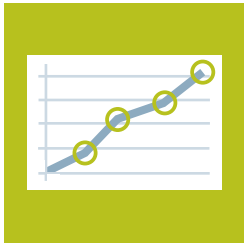
- **Control de Documentación**: bancos, cajas y entidades aseguradoras gestionan diariamente millones de documentos. Dicha gestión y manipulación documental genera un gran volumen de trabajo, espacio físico, logística e inversión de tiempo. Con la utilización de la solución **BeSign** de reconocimiento de firma biométrica al no ser necesaria la utilización de documentos en formato papel, se evitan errores, pérdidas, almacenaje y custodia, así como deterioro, disponiéndose la documentación en formato electrónico bajo control, en entorno seguro y accesible desde cualquier lugar en todo momento.

- **Reducción de costes y optimización de la productividad**: la firma biométrica permite una mayor agilidad y seguridad en el proceso de contratación, pudiendo firmar un mismo documento por diferentes personas en lugares y momentos distintos. Además, supone una disminución de pérdidas o errores operativos, con el consecuente ahorro de costes.

  En este sentido, tomando como ejemplo una entidad financiera de tamaño medio, con unos Activos Totales Medios de 85.000 M€, 1.300 oficinas y unos 55 millones de operaciones tramitadas al año, la estimación en reducción de costes sería:

  - Costes directos: eliminación de papel supondría **1,5 millones de euros**.
  - Eficiencia Operativa: reducción de **45.000 h**.
  - Ahorro en costes indirectos: **1.940.000 euros**.

- **Mejora/Reingeniería de procesos**: la evolución continua de la tecnología y la necesidad de desarrollar la implantación de proyectos que cubran la necesidades tanto internas de cada compañía como las expectativas de los clientes, son los mayores retos con los que se enfrentan a diario los responsables de los departamentos de TI. Con la automatización de procesos que ofrece la solución **BeSign** todas las tareas de firma, verificación, encriptación y archivo se realizan en el mínimo tiempo y siempre bajo control.



- **Imagen innovación tecnológica**: por tratarse de una tecnología de última generación, con dispositivos cada vez más ligeros, rápidos y seguros, y por transformar los procesos de trabajo, las empresas que evolucionan a esta tecnología ofrecen una verdadera imagen de modernidad e innovación.
- **Prevención del fraude**: gracias a la posibilidad de realizar la autenticación del firmante en el momento de la firma, ésta queda encriptada junto al documento almacenado y custodiado.
- **"Green Office"**: la eliminación de papel en los procesos de firma y la eliminación del uso de impresoras (tinta o tóner), ayudan a reducir el impacto medioambiental. Tomando como ejemplo una entidad financiera de tamaño medio el impacto medio ambiental se reduciría en la utilización de **110 millones** de hojas de papel menos, lo que supone no talar 14.903 árboles al año[4].
- **Aumento en la seguridad**: los documentos a firmar nunca residen en los dispositivos móviles; siempre residen en el servidor central. En el dispositivo móvil sólo aparece una "imagen" del documento y del documento firmado.

La solución **BeSign**, propiedad de **Serban**, utiliza un hardware específico, ya sea pantalla o pluma, para recoger una serie de información sobre la firma de los usuarios:

- Coordenada x
- Coordenada Y
- Presión que se ejerce (p)
- Instante de tiempo (t)

Esta información es procesada por **BeSign** en modo vectorial de todos los puntos del grafo de la firma: (<x,y,p,t><x,y,p,t><x,y,p,t><x,y,p,t><x,y,p,t><x,y,p,t><x,y,p,t>)

En función de la capacidad de recogida de presión del dispositivo o de la pluma, estos valores oscilan entre 0 y 524 o 0 y 1024.

Con esta información, los algoritmos propiedad de Serban, procesan estos datos para obtener ciertos datos biométricos de la firma.

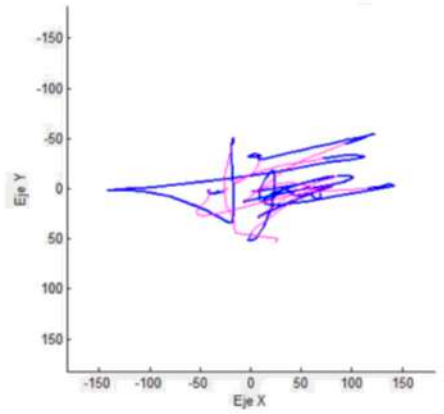
El algoritmo usa una combinación de técnicas basadas en **Hidden Markow Models** (Modelos Ocultos de Markow) y **Dinamic Time Warping** (Alineamiento Temporal Dinámico). Estos algoritmos se utilizan como métodos de reconocimiento de patrones y como métodos de medición de variación de variables a lo largo del tiempo o del espacio.

Los datos calculados por **CheckSign** para crear el patrón son los siguientes:

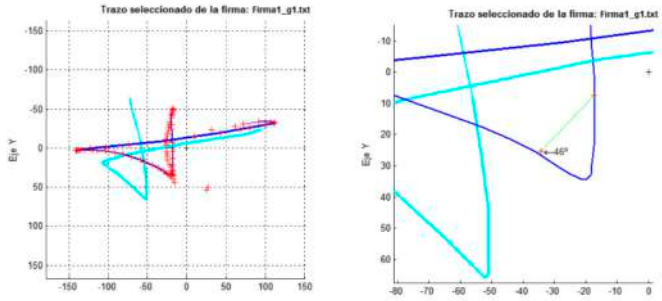
- Aceleración.
- Aceleración Delta.
- Velocidad.
- Velocidad delta.
- Velocidad en el eje de coordenadas X.
- Velocidad en el eje de coordenadas Y.
- Vuelo del lápiz.

A continuación, se muestran imágenes donde se muestran la obtención de rasgos característicos de la firma manuscrita:

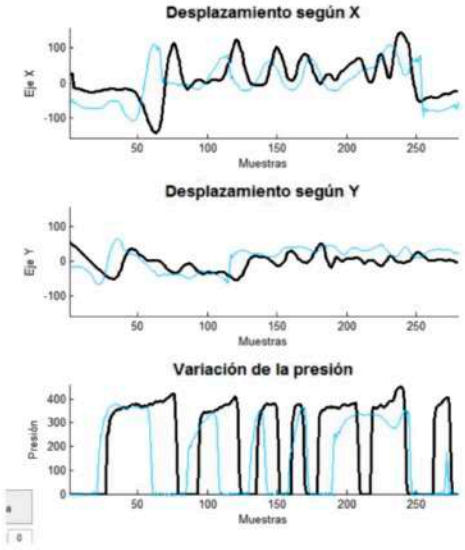
- Vuelo de la pluma durante el recorrido de la firma:



- Medición de ángulos en trayectorias



- Comparación de firmas, basándose en los desplazamiento en eje X y eje Y y la presión:



Esta información sobre las propiedades de una firma **no es visible en ningún momento**, ni para la Entidad ni para los actores intervinientes en el proceso.
Con estos datos se genera un **patrón biométrico** de la firma del usuario. Este patrón es utilizado por el producto **CheckSign,** propiedad de Serban, para realizar las comparaciones entre firmas y los patrones de los usuarios.
Con este patrón biométrico de firma, nunca en ninguna circunstancia se puede reconstruir el grafo de la firma ni se puede obtener información sensible de los usuarios.

Proceso de verificación de identidad

El proceso de verificación de la identidad de un usuario a través de su firma usando CheckSign, es el siguiente:

Lh 1>ǫ I 9KM>ǫ=>ǫNG9ǫ F N>LMK9ǫ=>ǫNG9ǫ?BK F 9ǫ K><H@B=9ǫ9ǫMK9O¦Lǫ=>ǫNGǫ=BL I HLBMBOHǫNMBEBS9G=Hǫ E9ǫLHEN<BæGǫ >1B@Gh̨ǫǫ

I·h "LM9ǫ F N>LMK9ǫ>Lǫ I KH<>L9=9ǫŦGHK F 9EBS9<BæGǫ=>ǫ O9EHK>Lǫ=>ǫ I K>LBæG‡ǫRǫL>ǫ>QMK9>GǫE9Lǫ <9K9<M>KÅLMB<9LǴǫM9EǫRǫ<H F HǫL>ǫBG=B<9ǫ>Gǫ>LM>ǫ =H<N F >GMHh̨ǫǫ

Łh "L9ǫ F N>LMK9ǫL>ǫ<H F I 9K9ǫ<HGMK9ǫ>Eǫ I 9MKæGǫ ;BH F ¦MKB<Hǫ=>EǫNLN9KBHǴǫ9ǫMK9O¦Lǫ=>ǫEHLǫ 9E@HKBM F HLǫ I KH I B>M9KBHLǫRǫL>ǫ=>ON>EO>ǫNGǫ K>LNEM9=Hh̨ǫǫ

Ńh - HKǫÐEMB F HǴǫ>EǫK>LNEM9=Hǫ>Lǫ>EǫL<HK>ǫ=>ǫE9ǫ <H F I 9K9<BæGǫJN>ǫE9ǫ"GMB=9=ǫ I H=KUǫNL9Kǫ I 9K9ǫ =>?BGBKǫE9LǫK>@E9Lǫ=>ǫG>@H<BHǫJN>ǫG><>LBM>h̨ǫǫ

Para más información:

Para saber más sobre **BeSign de Serban Biometrics**:
http://www.serbanbiometrics.es/es/soluciones/firma-digitalizada-biometrica

[1] Fuente: Banco Central Europeo (Europa Press 12/08/2013) www.europapress.es/economia/finanzas-00340/noticia-banca-cerro-1963-oficinas-espana-2012-357-total-eurozona-20130812120618.html

[2, 3 & 4] Fuente: Estudios realizados por Serban Biometrics.