Calidad de datos: ¿costo o inversión?

Por Alberto Collado, Director General
de PowerData para América Latina

La información que maneja una organización constituye una de sus principales ventajas competitivas sostenibles en el tiempo. Por eso, la calidad de la información corporativa se está convirtiendo en uno de los más acuciantes problemas para empresas de todos los tamaños y sectores ya que influye directamente en su productividad. Sin embargo, muchas de ellas no dedican aún suficiente atención a la calidad de la información que soporta sus decisiones.
La no calidad de la información - entendida como la ausencia de datos duplicados, erróneos, en formatos inadecuados, obsoletos o difícilmente accesibles- genera importantes pérdidas: desde el costo de envíos publicitarios a miles de direcciones erróneas o duplicadas, pasando por el fraude o el gasto en recursos dedicados a limpiar la información, hasta el desaprovechamiento de oportunidades de negocio o la toma de decisiones equivocadas. Según el Data Warehousing Institute, sólo en EE.UU. las pérdidas originadas por la mala gestión de los datos se estimaron en unos 600.000 millones de dólares en 2002.
Visto de otra forma: según algunos expertos, la mala calidad de Datos puede llegar a representar hasta el 20% de la facturación empresarial.

Sin embargo, como sucede con otros segmentos de las TI, la Calidad de los Datos es una de aquellas tecnologías de las que todos conocemos su existencia y utilidad, pero resulta difícil saber qué es exactamente lo que hay hacer o incluso por dónde empezar.
En primer lugar, porque los entornos de administración de negocios son cada vez más complejos y los datos se encuentran dispersos en múltiples aplicaciones: desde sistemas de gestión de relaciones con los clientes (CRM) hasta plataformas de planificación de recursos empresariales (ERP), data warehouse o BI. Una pobre calidad de los datos podrá por tanto provocar multitud de fallos en la cadena de suministro y conducir a decisiones de negocio inadecuadas, además de impedir la segmentación, análisis y visión única de los clientes.

Garantizar la calidad de los datos es una tarea difícil y compleja, que involucra a diversas áreas de la organización y que implica una decisión estratégica para la que no existe un producto mágico. Este enfoque integral ayuda a las empresas a ahorrar dinero y obtener un retorno de la inversión en menos de un año-, tomar decisiones de negocio más informadas –basadas en datos actualizados y oportunos-, ofrecer un mejor servicio al cliente a través de una visión unificada, agilizar la gestión de la cadena de suministro, entre muchas otras ventajas. Por eso, estamos convencidos de que la Calidad de Datos no debe verse como un costo, sino como una inversión.

PowerData

CONTACTO DE PRENSA

Muriel Mirvois
aleph.comunicacion@gmail.com
4556-1467 / 15 6106-6560
www.alephcom.es

¿Firma digital o firma electrónica?
La respuesta es animarse a innovar
Por Rodolfo Lomascolo, CEO de ipsCA y VP para Iberia - LatAm de STS Group

---

Que un ataque informático puede tener consecuencias graves para la organización, desde importantes pérdidas económicas hasta incluso poner en riesgo la continuidad del negocio ya no es una novedad. Y si se tiene en cuenta que el malware y los delitos digitales continúan en aumento, el panorama es preocupante. La lista de "amenazas" es larga: robo o suplantación de identidad, fraude financiero, robo o difusión de información sensible o confidencial, entre muchas otras.

En este contexto las herramientas de firma digital están experimentando un claro crecimiento en todo el mundo, ya que refuerzan la protección en el intercambio de datos y hasta permiten dotar a la información con valor probatorio.

Sin embargo y a pesar de sus múltiples ventajas, no es de las tecnologías más difundidas en la Argentina. De hecho, fuera de ciertos ámbitos de la administración pública, su nivel de adopción ha sido casi nulo, a pesar de los casi ocho años trascurridos desde la sanción de la ley que le otorgó el mismo status legal que a la firma manuscrita y a dos de establecido el marco normativo aplicable al otorgamiento y revocación de licencias para emitir certificados digitales.

Pero hace apenas unos días, AFIP dio a conocer una serie de medidas para agilizar y controlar el comercio, que seguramente cambiarán este panorama. Entre ellas se encuentran el uso de la firma digital en los contratos de compra-venta de granos - según explicó el titular del organismo, "será el primer contrato con firma digital entre privados**".** La entidad aprobó además la resolución 2651 mediante la cual establece el procedimiento para la emisión de certificados a los contribuyentes. Se trata sin duda de un avance importante y abre la posibilidad para que poco a poco las empresas comiencen a incorporar esta herramienta a sus procesos de negocio. Pero será una transición lenta.

En ese sentido, vale la pena mencionar que existe una gran confusión sobre que la firma electrónica (para lo que no se requiere un certificado asociado) tiene menos validez que la digital, una imprecisión que poco ha contribuido al despegue de estas tecnologías.

La realidad es que según **la Ley 25.506 ambas tienen valor legal**. **La diferencia radica en el valor probatorio de cada una**: en el caso de la **firma digital** existe una presunción "iuris tantum" en su favor; esto significa que se presume salvo prueba en contrario por parte del demandante que proviene del suscriptor del certificado asociado. **En la firma electrónica se invierte la carga de la prueba**: en caso de ser desconocida una firma, corresponde a quien invoca su autenticidad acreditar su validez. Por ejemplo, si A y B celebran un contrato firmado digitalmente y A alegara la invalidez de alguna de las firmas, le corresponde a A demostrarlo ante la ley. Si en cambio, el contrato se hiciera con firma electrónica, corresponde a la parte que asugura su autenticidad demostrarlo ante la ley y sólo en caso de no poder probarla, esa firma electrónica se considera inválida.

Nuestra experiencia en Europa indica que un factor importante para el despegue de la firma digital fue el incetivo del estado (por ejemplo, beneficiendo con devoluciones de impuestos en menor tiempo a quiener utilizaban los medios electrónicos). Pero sin duda lo que dio el impulso definitivo fue que el sector privado comenzar a incorporar a sus procesos de negocio las tecnologíasde firma para replicar en digital los procedimientos que se hacían en papel, manteniendo toda su integridad y validez. En nuestros 15 años de experiencia no ha habido ningún caso de repudio que haya llegado a un tribunal y que sepamos, en Europa no se ha dado esa situación.
Y esto puedo lograrse tanto con la firma digital como con la electrónica.

De hecho, las principales cámaras argentinas del sector TI han llamado la atención sobre la eficacia de la firma digital en varios capítulos del documento "Bases y lineamientos para una Agenda Digital Argentina". Pero también menciona que "si bien se ha avanzado en la materia, existen aplicaciones que utilizan métodos alternativos de autenticación en forma exitosa y que están siendo utilizadas masivamente sin generar repudio de transacciones".

Argentina y Latinoamérica en general tienen la ventaja de comenzar a incorporar una tecnología ya muy probada y extendida en otros sitios. Se trata, en definitiva, de "perder el miedo", a ser los primeros, a innovar. Los beneficios son muchos y están sólo un paso más adelante.

Datos sucios: un enemigo invisible

Por Alberto Collado,
Director General de PowerData para América Latina

Envíos publicitarios a direcciones erróneas o duplicadas, oportunidades de negocio desaprovechadas, toma de decisiones equivocadas porque los datos no estaban disponibles o eran incorrectos… La calidad de los datos está estrechamente relacionada con la falta de flexibilidad de algunos sistemas informáticos y con los errores y negligencias humanas. Los datos, de hecho, deben lograr un continuo equilibrio entre la rapidez y la agilidad que demandan los ejecutivos, y los límites de la estructura tecnológica.

Los departamentos de marketing en particular suelen trabajar con un gran número de bases de datos, con múltiples registros del mismo cliente, que es necesario cruzar, limpiar, combinar y ordenar para obtener una visión única y unificada de cada uno los clientes actuales o potenciales, para dirigirse a ellos con mayor eficacia y amoldándose a sus necesidades.

Cuando una empresa atiende debida y oportunamente a la calidad de sus datos, las campañas de marketing son más efectivas: se reduce el porcentaje de correo que no llega a su destino y se eliminan los registros duplicados. Pero los envíos repetidos generan otro importante problema, quizá mucho más grave que los costos económicos: la mala impresión que se causa. Cada vez que una compañía se dirige a un cliente como si todavía no lo fuera, o intenta venderle dos veces el mismo producto o le envía por enésima vez el mismo catálogo, la imagen y credibilidad de esa empresa se deteriora. Los clientes cada vez son más conscientes de su valor y sus derechos y esperan que se los entienda y conozca. La soluciones de calidad de datos ayudan a lograr ese resultado ya que permite n identificar a los miembros de un mismo hogar o empresa para dirigirse a ellos de forma adecuada.

Por otro lado, los datos con los que cuenta una empresa determinan el éxito o fracaso de un proyecto. Y para que esos datos sean fiables es necesario contar con plataformas potentes, flexibles y escalables para la integración, consolidación, migración, sincronización y almacenamiento de los datos. Más a delante serán necesarias herramientas de evaluación (perfilado de datos), de análisis, de categorización y de estandarización, para llegar finalmente a las etapas de corrección o limpieza, mejora, cruce de datos, consolidación y *reporting*.

La posibilidad de no acertar con la estrategia adecuada o perder oportunidades por no contar con los datos son motivos más que suficientes para que las empresas –más allá de su tamaño- se plantee seriamente si cuenta con la información actualizada y fiable que su negocio necesita.

¿Sabía qué…?

- El gasto total en integración de datos aumentará aproximadamente desde los 9,3 billones de dólares en 2003 hasta los 13,6 billones en 2008 (Previsión de gastos en integración de datos a nivel mundial para el período 2004-2008 de IDC, julio de 2004)
- Algunos analistas del sector estiman que el mercado global para las soluciones de calidad de la información crecerá un 12% anual hasta alcanzar el billón de dólares en 2008
- El costo de la mala calidad de los datos puede llegar a representar hasta el 20% de la facturación empresarial., según algunos expertos,
- *Según Gartner, más de 25% de los datos críticos de las empresas Fortune 1000 es erróneo, incompleto o de mala calidad, y por eso muchas compañías toman decisiones equivocadas.*

PowerData

CONTACTO DE PRENSA

Muriel Mirvois
muriel@alephcom.com.ar
4556-1467 / 15 6106-6560
www.alephcom.es

El peligro de los *datos sucios*

Muchas empresas lo ven como un costo en lugar de una inversión, pero la mala calidad de los datos puede significar pérdidas millonarias.

Por Alberto Collado, Director General
de PowerData para América Latina

Disponer de una versión única y accesible de la información es una cuestión cada día más crítica para las empresas. Con el exponencial crecimiento de los datos en los últimos años, ha crecido también la presencia de datos incorrectos, incompletos, incoherentes o desactualizados en las diferentes bases de datos y aplicaciones empresariales. Como consecuencia, las organizaciones se enfrentan en ocasiones a un gran volumen de *datos sucios* que entorpecen la toma de decisiones, dañan su imagen en el mercado y pueden ocasionarles pérdidas millonarias.

Calcular el costo directo de la no calidad de los datos es en algunos casos bastante sencillo. Veamos algunos ejemplos. El segundo grupo bancario japonés, Mizuho, perdió exactamente 286 millones de euros por un error tipográfico. En diciembre de 2005, tras la salida a bolsa de una pequeña sociedad, J-Com, un corredor de este banco había puesto 610.000 títulos a 1 yen, en lugar de vender 1 título a 610.000 yenes. El error, que no pudo ser reparado a tiempo por los servicios informáticos de la Bolsa de Tokio (TSE), le costó además el empleo al jefe de TSE, Takuo Tsurushima, quien dimitió un mes más tarde.

En 1999, la NASA perdió el satélite Mars Climate Orbiter a causa también de datos erróneos. De hecho, el satélite fue destruido durante su puesta en órbita en Marte a una altitud de 50 kilómetros de la superficie (la altitud prevista normalmente era de 150 kilómetros) por las turbulencias y las fricciones atmosféricas. La investigación puso en evidencia que ciertos parámetros habían sido calculados en unidades de medición anglosajonas, y transmitidos tal cual al equipo de navegación, que esperaba estos datos en unidades del sistema métrico. Este “pequeño” error costó 125 millones de dólares a los contribuyentes norteamericanos.

En otras ocasiones, la introducción de los datos directamente por parte del cliente puede tener también consecuencias inesperadas. En algunas webs de turismo y viajes, es posible reservar en Internet un vuelo de ida y vuelta ¡con la fecha de retorno previa a la fecha de salida! Hay que ser realmente despistado para hacer una reserva así, pero ¿el control de la validez de la propuesta no es responsabilidad de las compañías aéreas? También podríamos preguntárselo a

los tres clientes noruegos de una compañía aérea que les envió al municipio francés de Rodez cuando ellos querían pasar sus vacaciones en la isla griega de Rodas. Otro caso revelador es el de una gran compañía de seguros que había decidido fusionar sus bases de datos para tener un conocimiento más global sobre su cartera de clientes y los productos que pudiesen interesar a cada segmento, mejorando así los servicios prestados. Antes de iniciar el proyecto, la dirección pensaba que tenía 13 millones de clientes, una estimación basada en las informaciones de las que disponían. Tras la fusión de las bases de datos, descubrieron muchos registros duplicados en las bases de datos, lo que redujo nada menos que en cinco millones el número real de clientes de la compañía.

Vistos estos ejemplos, no cabe duda de que la calidad de los datos debe ser un requisito esencial en las estrategias corporativas, apoyándose en la tecnología existente de limpieza e integración de datos para que los datos sucios queden fuera de nuestros activos de información.

Box
¿Sabía qué…?

- El gasto total en integración de datos aumentará aproximadamente desde los 9,3 billones de dólares en 2003 hasta los 13,6 billones en 2008 (Previsión de gastos en integración de datos a nivel mundial para el período 2004-2008 de IDC, julio de 2004)
- Algunos analistas del sector estiman que el mercado global para las soluciones de calidad de la información crecerá un 12% anual hasta alcanzar el billón de dólares en 2008
- El costo de la mala calidad de los datos puede llegar a representar hasta el 20% de la facturación empresarial., según algunos expertos,
- *Según Gartner, más de 25% de los datos críticos de las empresas Fortune 1000 es erróneo, incompleto o de mala calidad, y por eso muchas compañías toman decisiones equivocadas.*

Validez de la prueba electrónica: cómo superar la inseguridad jurídica
(Primera parte)
Por Rodolfo Lomascolo, CEO de ips*CA* y VP para Iberia y LatAm de STS Group

Si bien es cierto que poco a poco los países comienzan a adaptar su marco jurídico a las nuevas tecnologías en general, y a los hoy imprescindibles intercambios de información digital en particular, aún subsisten dudas en cuanto a las pruebas electrónicas.

Es por ello que en una instancia judicial la admisibilidad de un conjunto de datos como prueba dependerá del soporte en el que se presente. Y si bien la prueba digital es admitida, en la mayoría de los tribunales del mundo se da mayor validez a la evidencia impresa. Existe un enorme recelo frente a las nuevas tecnologías por lo que en general la prueba electrónica no es considerada plena.

Este vacío legal en materia de prueba electrónica hace que el derecho a presentar este tipo de evidencias quede supeditado al criterio del magistrado en cuestión. En consecuencia, los abogados prefieran presentar pruebas impresas, generándose un círculo vicioso que no es fácil modificar.

Por su naturaleza, la prueba electrónica es fácilmente manipulable; no solo los documentos pueden ser alterados: incluso debe poder demostrarse de forma fehaciente que la información reúne las características de *perdurabilidad e inalterabilidad,* incluso de aquellos documentos que no han sufrido modificaciones.

Pero la admisibilidad de una evidencia digital no sólo está asociada a su integridad. Otro aspecto importante es que en muchos casos la prueba es de tipo unilateral (solo se encuentra en posesión de una de las partes), por lo que se vuelve vital la conservación y la salvaguarda de toda la cadena de custodia.

Y no debemos olvidar el carácter transnacional de los tráficos de datos: en muchos casos intervienen servidores ubicados en países con legislaciones diferentes.

Las terceras partes de confianza (como ¿???? citar algún/os ejemplos) representan una solución, proporcionando servicios que aseguren que dichas pruebas electrónicas sean perdurables e inalterables.

No cabe duda de que el incremento exponencial de los intercambios electrónicos requiere una urgente actualización de las leyes, así como la adopción de todas las normas internacionales relacionadas con la custodia y retención de información digital. Pero igualmente cierta es la necesidad de definir, diseñar, desarrollar, utilizar y auditar sistemas de preservación de pruebas electrónicas.

Los peritos, pieza fundamental en los procesos judiciales, solo deberían intervenir en casos dudosos. Y las pruebas tienen que provenir de sistemas eficaces para proteger la integridad de la evidencia electrónica y de toda la cadena de custodia, de modo que su aceptación sea inequívoca.

En ese sentido, la utilización de sistemas que no puedan asegurar íntegramente

la cadena de custodia crean un clima de desconfianza, desfavorable para las pruebas electrónicas.

Por todo lo expuesto, es aconsejable que los departamentos de TI de las empresas, y en particular los responsables de seguridad, comiencen a analizar sus necesidades de custodia de información probatoria, en función de las exigencias de su negocio, para evitar la inseguridad jurídica.

SEGUNDA PARTE (VERSIÓN FINAL DE RLo-.Enviado a Dra. Davara 29-20-09)

Validez de la prueba electrónica: cómo superar la inseguridad jurídica

(Segunda parte)
Por Rodolfo Lomascolo, CEO de ips*CA* y VP para Iberia y LatAm de STS Group

Requisitos de las soluciones de custodia a efectos probatorio

Las soluciones de archivo probatorio, concebidas por razones legales y reglamentarias, requieren una conformidad con la normativa y una capacidad de respuesta a las exigencias reglamentarias.

Donde las leyes no cubren los aspectos relativos al almacenamiento de pruebas electrónicas, las normas juegan un papel importante dado que ellas representan “el estado del arte” y la aportación de los expertos en la materia.

El archivo electrónico representa un perímetro amplio, ya que está asociado al ciclo de vida del documento o de los datos, y las normas y modelos existentes no cubren totalmente este perímetro.

Es importante conocer el universo normativo colocando las normas relacionadas con el archivado electrónico en un mapa de utilización
Normas relacionadas con el archivado electrónico:

- MOREQ 2. Especificación del Modelo de Requisitos para la Gestión de Registros Electrónicos
- ISO 10006. Sistemas de gestión de calidad – Líneas directrices para la gestión de la calidad en los proyectos
- ISO 14721. Open Archival Information System (OAIS)
- ISO 15489. Información y documentación «Gestión de Registros»
- - parte 1 « Principios directores» y
  - parte 2 « Guía práctica » (ficha n°5 bis)
- ISO/CEI 27001. Tecnologías de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Exigencias y Requisitos
- ISO/CEI 27002. Tecnologías de la información – Técnicas de seguridad – Código de buena práctica para la gestión de la seguridad de la información
- ISO/CEI 27005. Tecnologías de la información – Técnicas de seguridad – Gestión del riesgo en seguridad de la información.
- ISO 23081. Información y documentación – Proceso de gestión de los registros – Metadatos para los registros.

El modelo OAIS (Open Archival Information Systems)

OAIS, modelo de referencia, fue desarrollado por el Consultative Committee for Space

Data Systems (CCSDS), para proporcionar un entorno para la estandarización de la preservación de objetos de todo tipo en el entorno científico.

OAIS fue creado con el objetivo de ser ampliamente aplicado para la preservación a largo plazo de cualquier tipo de objeto, no exclusivamente de objetos digitales. El modelo OASIS existe en un nivel de abstracción general, proporcionando un entorno que responde a los requerimientos de conservación a largo plazo, independiente de la implementación que se realice.

En el modelo OAIS es importante la creación de una terminología común para definir los procesos, los métodos y los objetos.

Preservación a largo plazo

La preservación de la información es un desafio significativo para los responsables de la retención de información. OAIS es muy claro en su objetivo de preservación a largo plazo. La mayoría de sistemas de almacenamiento actuales no pueden decir que su objetivo principal se la preservación de la información. Tampoco las empresas que realizan almacenamiento de información con el objetivo de utilizarla con valor probatorio pueden decir que sus sistemas estén pensados en base a una preservación a largo plazo o incluso indefinida.

Cualquier repositorio de información debería considerar la importancia de la preservación de la información, y OAIS es el modelo ideal para realizar esta preservación de una forma organizada o coherente.

La Digital Preservation Coalition define la preservación digital como: “la serie de actividades organizadas necesarias para asegurar la continuidad en el acceso a la información digital durante el tiempo que sea necesario”, OAIS define que “el largo plazo puede extenderse indefinidamente” (CCSDS 2002, p. 1-1).

Esta flexibilidad en definir la duración temporal no es ninguna ventaja para los repositorios digitales con valor probatorio, ya que no se puede planificar un sistema fiable si no se puede basar en una norma que defina correctamente las duraciones temporales.

Un aspecto importante en la preservación a largo plazo es la poca experiencia existente a día de hoy en este tipo de actividad, el gran número de interrogantes existentes respecto a las amenazas futuras que se pueden presentar par la información custodiada además del equilibrio que se tiene que tener entre la actividad e custodia fiable con la necesidad de cargar la información en los repositorios.

OAIS acepta que las actividades relacionadas con la preservación a largo plazo puede entrar en conflicto con los objetivos de introducción y diseminación de los productos y servicios a los consumidores (CCSDS 2002, p. 2-1).

PARTE 2

Algunos comentarios/ Observaciones y preguntas

1) Las soluciones de archivo electrónico deberían cumplir con TODAS esas normas que detallamos o puede inclinarse sólo por una/algunas?
2) Por qué desarrollamos sólo OAIS y no el resto?
3) Si la idea es decir que lo mejor es seguir OAIS, me parece que deberíamos analizarlo un poco más y explicar/fundamentar mejor por qué afirmamos eso…
4) Qué es eso de las fichas? (estoy navegando la web de iso, pero no está fácil encontrarlas, además de que no se pueden consultar si no las compras…)
5) Si hablamos de un "mapa de utilización" (de las normas disponibles) estaría bueno explicar brevemente por qué (según nuestra opinión) inclinarse por unas en lugar de otras.

http://www.iso.org/iso/home.htm

Sobre moreq 2: *"Model Requeriments for The Management of Electronic Records"*presentadas a la Unión Europea en el año 2001.

TEXTO ORIGINAL

PARTE UNO

La prueba electrónica

Desde hace varios años, el desarrollo de la desmaterialización en general y del archivado electrónico en general, ha generado la necesidad de normas destinadas a permitir definir, diseñar, desarrollar, utilizar y auditar sistemas de preservación de pruebas electrónicas. Aunque a día de hoy existe discrimación clara de la prueba electrónica frente a otros tipos de pruebas tradicionales. La admisibilidad de un conjunto de datos como prueba dependerá del soporte sobre e que se presente, y en la mayoría de tribunales del mundo se da mayor validez a la prueba impresa que a la prueba electrónica. El factor fundamente de esta discriminación es la falta de una legislación específica referente a la prueba electrónica y la enorme desconfianza de los juzgados en lo que afecta a las nuevas tecnologías.

La prueba electrónica no es en general prueba plena, en contraposición a la prueba en papel.

Todo esto nos lleva a afirmar que la falta de legislación en materia de prueba electrónica hace que el derecho a presentar pruebas electrónicas quede siempre bajo tutela judicial, donde la aceptación depende totalmente del jucio del magistrado en cuestión. Esto lleva a que los abogados prefieran presentar las pruebas electrónicas en formato papel, una vez impresas, con todas las consecuencias que implica esto.

Está claro que es necesaria una modificación de las actuales leyes, y la adopción de toda la serie de normas internacionales que están relacionadas con la custodia y retención de información digital.

La prueba electrónica, por su propia naturaleza es volátil y fácil de ser manipulada,

por lo que es necesario protegerla de forma que pueda ser aceptada de forma inequívoca.

La preservación de la integridad de la prueba electrónica y de la cadena de custodia deben ser el objetivo principal de los sistemas de retención y custodia que pretenden mantener el archivo de este tipo de datos.

Los peritos, de ayuda fundamental para resolver los procesos judiciales, deberían intervenir solo en aquellos casos que generen dudas, y las pruebas deberían provenir de sistemas de custodia que aseguraran esta integridad y cadena de custodia.

La inseguridad jurídica generada por sistemas que no cumplen las necesarias medidas de seguridad produce que no se cree un entorno favorable para las pruebas electrónicas.

No solo los documentos pueden ser alterados, sino que incluso con documentos que no han sufrido alteración, se debe poder demostrar de forma fehaciente que la información, volátil por naturaleza, reúne las características de *perdurabilidad e inalterabilidad.*

Las terceras partes de confianza pueden representar una solución para proporcionar servicios que seguren que dichas pruebas electrónicas sean perdurables e inalterables

Otro aspecto importante es la uniteralidad de la prueba electrónica, incluso teniendo mucha importancia el aspecto transnacional de los tráficos de datos, donde intervienen en muchos casos servidores que se encuentran en países con legislaciones diferentes.

La admisibilidad de la prueba electrónica está asociada a su conservación, y la salvaguarda de la cadena de custodia es fundamental, dado que las pruebas electrónicas en muchos casos son de tipo unilateral, estando en posesión solo de una de las partes.

Los departamentos de sistemas de las empresas deberían comenzar a analizar sus necesidades de custodia de información probatoria, en función de las exigencias de su negocio. Los responsables de Seguridad deberían analizar las necesidades de retención estableciendo mecanismos que aseguren la custodia y la cadena de custodia.

PARTE 2

Requisitos de las soluciones de custodia a efectos probatorio

Las soluciones de archivo probatorio, concebidas por razoles legales y reglamentarias, requieren una conformidad con la normativa y una capacidad de respuesta a las exigencias reglamentarias.

Donde las leyes no cubren los aspectos relativos al almacenamiento de pruebas electrónicas, las normas juegan un papel importante dado que ellas representan “el estado del arte” y la aportación de los expertos en la materia.

El archivo electrónico representa un perímetro amplio, ya que está asociado al ciclo de vida del documento o de los datos, y las normas y modelos existentes no cubren totalmente este perímetro.

Es importante conocer el universo normativo colocando las normas relacionadas con el archivado electrónico en un mapa de utilización
Normas relacionadas con el archivado electrónico :

· Fiche n° 2 : MOREQ 2. Model Requirements Specification for the Management of Electronic Records

· Fiche n° 3 : ISO 10006. Systèmes de management de la qualité – Lignes directrices pour le management de la qualité dans les projets

· Fiche n° 4 : ISO 14721. Open Archival Information System (OAIS)

· Fiche n° 5 : ISO 15489. Information et documentation « Records Management »
- partie 1 « Principes directeurs » et
- partie 2 « Guide pratique » (fiche n°5 bis)

· Fiche n° 6 : ISO/CEI 27001. Technologies de l'information - Techniques de sécurité - Systèmes de gestion de la sécurité de l'information - Exigences (Information Technology – Security techniques – Information security management systems – Requirements)

· Fiche n° 7 : ISO/CEI 27002. Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour la gestion de la sécurité de l'information

· Fiche n° 8 : ISO/CEI 27005. Technologies de l'information - Techniques de sécurité - Gestion du risque en sécurité de l'information ; entrera en révision à la sortie de la 31000

· Fiche n° 9 : ISO 23081. Information et documentation -- Processus de gestión des enregistrements -- Métadonnées pour les enregistrements.

PARTE 3

El modelo OAIS

OAIS, modelo de referencia, fue desarrollado por el Consultative Committee for Space Data Systems (CCSDS), para proporcionar un entorno para la estandarización de la preservación de objetos de todo tipo en el entorno científico.

OAIS fue creado con el objetivo de ser ampliamente aplicado para la preservación a largo plazo de cualquier tipo de objeto, no exclusivamente de objetos digitales. El modelo OASIS existe en un nivel de abstracción general, proporcionando un entorno que responde a los requerimientos de conservación a largo plazo, independiente de la implementación que se realice.

En el modelo OAIS es importante la creación de una terminología común para definir los procesos, los métodos y los objetos.

Preservación a largo plazo

La preservación de la información es un desafio significativo para los responsables de la retención de información. OAIS es muy claro en su objetivo de preservación a largo plazo. La mayoría de sistemas de almacenamiento actuales no pueden decir que su objetivo principal se la preservación de la información. Tampoco las empresas que realizan almacenamiento de información con el objetivo de utilizarla con valor probatorio pueden decir que sus sistemas estén pensados en base a una preservación a largo plazo o incluso indefinida.

Cualquier repositorio de información debería considerar la importancia de la preservación de la información, y OAIS es el modelo ideal para realizar esta preservación de una forma organizada o coherente.

La Digital Preservation Coalition define la preservación digital como: “la serie de actividades organizadas necesarias para asegurar la continuidad en el acceso a la información digital durante el tiempo que sea necesario”, OAIS define que “el largo plazo puede extenderse indefinidamente” (CCSDS 2002, p. 1-1).

Esta flexibilidad en definir la duración temporal no es ninguna ventaja para los repositorios digitales con valor probatorio, ya que no se puede planificar un sistema fiable si no se puede basar en una norma que defina correctamente las duraciones temporales.

Un aspecto importante en la preservación a largo plazo es la poca experiencia existente a día de hoy en este tipo de actividad, el gran número de interrogantes existentes resptecto a las amenazas futuras que se pueden presentar par la información custodiada además del equilibrio que se tiene que tener entre la actividad e custodia fiable con la necesidad de cargar la información en los repositorios.

OAIS acepta que las actividades relacionadas con la preservación a largo plazo puede entrar en conflicto con los objetivos de introducción y diseminación de los productos y servicios a los consumidores (CCSDS 2002, p. 2-1).

La amenaza de los datos sucios

Por Alberto Collado,
Director General de PowerData para América Latina

Faltas ortográficas, códigos y abreviaturas incorrectas, datos desfasados… Todos estos pequeños errores pueden convertirse en pérdidas millonarias. La calidad de los datos que maneja una organización –tanto una gran corporación como una pequeña empresa- se ve constantemente amenazada por situaciones tan comunes como una migración de base de datos, la nueva situación del cliente del que tomamos los datos (un cambio de domicilio, un divorcio e incluso el fallecimiento), el traspaso de información de una aplicación a otra…

No dedicar la suficiente atención a la reconciliación e integración de los datos dará lugar a un peligroso fenómeno para nuestro negocio: los datos sucios. Las empresas invierten grandes sumas de dinero en , por ejemplo, aplicaciones CRM para la gestión de sus relaciones con los clientes. Sin embargo, si los datos de origen no se actualizan, cuando el departamento de marketing utilice esa base de datos para lanzar una campaña, malgastará miles de pesos en envíos postales a direcciones que no existen o están duplicadas. Por no hablar de los riesgos de fraude y robo de identidad, que darán lugar a posibles demandas y cuantiosas multas por parte de las entidades reguladoras.

Ante el constante envejecimiento de los datos, las empresas deben analizar y limpiar cuidadosamente sus datos antes de almacenarlos, incorporarlos a un sistema ERP o proceder a un proyecto de consolidación. La “suciedad” de los datos manchará inevitablemente la imagen de la empresa, generará desconfianza en sus clientes y proveedores y podrá conducir a decisiones equivocadas y a la pérdida de oportunidades de negocio.

PowerData

CONTACTO DE PRENSA

Muriel Mirvois
aleph.comunicacion@gmail.com
4556-1467 / 15 6106-6560
www.alephcom.es

Un enfoque cualitativo

Por Alberto Collado, Director General
de PowerData para América Latina

Aún mucho antes de que las computadoras se tornaran una herramienta indispensable para cualquier negocio y mucho antes también de que los modernos modelos de gestión empresarial fueran bautizados, era común creer que la clave para la toma de mejores decisiones era manejar cada vez más datos.

Pero en la “era de la información”, si hay algo que sobra son datos. De hecho, la cantidad de información que produce activamente un individuo ya fue superada por la “sombra digital”, es decir, todos los ceros y unos que se generan sin nuestra intervención directa: nombres en listas de *mailings*, búsquedas en la web, imágenes obtenidas por cámaras en la vía pública, etc. Este gran “universo digital” seguirá creciendo y cada vez será más importante procesarlo y analizarlo en menor tiempo.

En este contexto, la simplificación comienza a resultar indispensable y gana terreno un enfoque diferente sobre el valor de los datos: el que privilegia la calidad sobre la cantidad. Desde esta perspectiva, **los sistemas EPM (Enterprise Performance Management), así como muchos otros entornos relacionados con la inteligencia de negocios, serán tan buenos y efectivos como los datos que recogen. Sólo con datos fiables, consistentes y oportunos se logra dar verdadero valor a la información.**

A paso lento pero seguro, las organizaciones comienzan a entender que sus datos y los sistemas que los utilizan deben responder a exigentes patrones de calidad. Los datos son el reflejo de las actividades de la compañía, una de sus caras, y por tanto deben cumplir con los niveles de veracidad, exactitud, coherencia y validez que quiere dar la compañía. Por eso, la **Calidad de Datos** debe percibirse como una inversión y no como un costo. Aquellas compañías que no dediquen suficiente atención a la calidad de la información que soporta sus decisiones estratégicas de negocios pueden desaprovechar oportunidades o malgastar tiempo y dinero.

No existe ninguna otra iniciativa en las empresas que involucre a más personas que la gestión de la calidad de datos, ya que todos, en alguna parte del proceso, deben contribuir a garantizarla.

Firma electrónica en la nube: más seguridad para los negocios

Por Rodolfo Lomascolo, CEO de ipsCA y VP para Iberia - LatAm de STS Group

Las tecnologías de firma electrónica y certificados digitales están experimentando un claro crecimiento en todo el mundo. Y mientras que en algunos países –como España- ha alcanzado una amplia penetración, en Latinoamérica su adopción es todavía lenta.

En este sentido resulta más que auspiciosa la reciente aprobación por parte de la ALDF de la Ley de Firma y Medios Electrónicos en el ámbito del Distrito Federal. Este nuevo instrumento tendrá validez jurídica en documentos oficiales, notariales, administrativos o judiciales, así como los emitidos por particulares. Y si bien la secretaría de Desarrollo Económico será la encargada de promover su uso generalizado dentro de los procesos de negocios de las empresas establecidas en el D.F., la experiencia indica que las propias empresas tienen un papel fundamental para darle empuje a la adopción de estas tecnologías.

De probada eficacia, su utilización representa enormes ventajas como herramienta de seguridad en todo tipo de intercambios digitales (comercio electrónico, e-administración, identidad digital, etc.), así como la posibilidad de agilizar y modernizar procesos en un amplio abanico de segmentos: bancos, aseguradoras, colegios y consejos profesionales, administración pública, grandes, pequeñas y medianas empresas, así como particulares y profesionales.

Sus entornos de aplicación son múltiples:
-Factura electrónica
-Firma de contratos
-Workflows internos con firma
-Formularios electrónicos
-Comercio electrónico seguro
-Banca electrónica segura
-Archivado de documentos con valor probatorio
-Registro y gestión de documentos para ingenieros, arquitectos, abogados, contadores, escribanos, etc.
-Contratos de trabajo temporal / e-nómina
-Tasaciones
-Créditos, microcréditos, hipotecas
-Pólizas de seguro
-Voto electrónico
-Desmaterialización certificada de documentos y archivos
-Presentación de Balances y Cuentas
-Certificados catastrales
-Historia clínica digital

Sin embargo, a pesar de sus múltiples ventajas, muchas empresas que, bien por su infraestructura o por requerir esta tecnología sólo en momentos puntuales, no se inclinan por implementar un sistema de este tipo.

Pero la famosa “nube” abre nuevas posibilidades. El Software como Servicio (SaaS, por sus siglas en inglés) se presenta como otro camino para recortar gastos, así como la posibilidad para las PYMES de acceder a aplicaciones robustas o world class a costos razonables. Lo mismo para compañías que por su naturaleza no están interesadas en montar una infraestructura de TI.

La firma electrónica en formato SaaS permite a las empresas pagar únicamente por cada documento que necesiten firmar digitalmente, o como soporte de seguridad para otras aplicaciones.

Como es sabido, en el modelo SaaS *o* de “pago por uso” el usuario accede a servicios y aplicaciones a través de Internet, con lo que elimina la necesidad de adquirir licencias, gestionar la infraestructura y preocuparse por el mantenimiento y actualización. Esto implica rápida adopción, costos iniciales reducidos, actualizaciones sencillas; integración perfecta en la infraestructura TI existente, mayor ROI, fácil distribución, portabilidad y escalabilidad (los usuarios pueden estar distribuidos en sitios remotos y acceder en cualquier momento al sistema tan sólo con una conexión a Internet). En definitiva, permite a la empresa enfocarse en sus objetivos de negocio y no en manejar sistemas.

Pero a pesar de sus bondades muchas organizaciones se muestran renuentes a implementar esta modalidad porque consideran riesgoso delegar el control y administración de su información y datos sensibles a terceros. Y la

preocupación no es infundada: toda esta arquitectura multiusuario requieren prestar especial atención a la seguridad, tanta o más que la que se dedica a los sistemas internos.

En este contexto, la firma electrónica y los certificados digitales también ofrecen un enorme potencial, como el complemento perfecto para controlar y gestionar identidades y privilegios, garantizando la seguridad y confidencialidad. Tanto en Europa occidental como en EEUU, el mercado muestra una clara tendencia en esa dirección, mientras que en Latinoamérica y los países del este todavía predomina el enfoque tradicional. Pero hoy tienen la posibilidad de dar un verdadero salto tecnológico.

Estamos en un punto en el que el mercado TI, es más competitivo, en calidad, seguridad y reducción de costes y tiempo. Al juntar estas vertientes encontramos en el modelo SaaS y su aplicación para la e-firma una solución viable para que las empresas le den un valor añadido a sus servicios.

Acerca de ipsCA

Ips Certification Authority (ipsCA) es líder en la fabricación de herramientas de firma y facturación electrónica, además de pionera en Europa como Autoridad Certificadora. En abril de 2009 pasó a formar parte del grupo francés STS, integrando el intercambio y archivo de documentos electrónicos con valor probatorio a su amplia gama de soluciones, entre las que destacan la firma y facturación electrónica; certificación y visado digital, identidad digital, formularios telemáticos; voto y compulsa electrónica. Las herramientas de ***ipsCA*** *destacan por su optimizado diseño, rápida implementación, y compatibilidad con sistemas de identidad digital y DNI electrónico. En la actualidad la compañía dispone de productos de escritorio, aplicaciones para servidores y appliance plug & play que, basados en arquitectura SOA, aúnan toda la propuesta tecnológica de firma electrónica desarrollada por la empresa hasta la fecha.* ***IpsCA*** *mantiene acuerdos con más de 350 socios y partners internacionales, como Adobe, Microsoft –ipsCA es Autoridad Certificadora Raíz para todos los productos de la firma americana–, Sun Microsystems, IBM, Safenet, ActivIdentity, HP, Indra y Xerox, entre otros.*

Acerca de Grupo STS

Grupo STS *nace en el año 2000 como empresa fabricante de software. Sus oficinas centrales están localizadas en Rueil Malmaison (París) y Nîmes. Líder europeo en el intercambio y archivo electrónico con valor probatorio, la compañía está instalada también en España, Italia y Bélgica.Grupo STS cotiza en la Bolsa de Paris y en el Mercado Libre EURONEXT desde noviembre de 2005. Las soluciones de STS aportan un gran valor añadido y han ayudado a más de 250 clientes a adaptarse a las nuevas exigencias del mundo electrónico.*

LAS SOLUCIONES Y HERRAMIENTAS DE ipsCA-STS Group ESTÁN DISPONIBLES EN MÉXICO A TRAVÉS DE CLEVER SERVICES.

aleph comunicación
Muriel Mirvois
Coordinadora de cuentas
Argentina: 4781-9058 / 15 6106-6560
México: 55 8421-8412
muriel@alephcom.com.ar
www.alephcom.es

Empresa: ipsCA
Caso de éxito: Colegio de Ingenieros de Caminos, Canales y Puertos de España (CICCP)
Medio: CXO
Edición: Jul-Ago 08
PARA RELACIONAR CON: NOTA SOBRE CONGRESO DE FIADI (PEDIDO OSCAR)

Firma digital para colegios profesionales: ahorros millonarios

10 millones *de planos pasan cada año por el Colegio de Ingenieros de Caminos, Canales y Puertos de España. Toneladas de papel que se imprime, encuaderna, envía, revisa y coteja. Y sobre los que hay que estampar, uno por uno, el sello de goma del Colegio. Gracias a la firma digital y a la tecnología Acrobat PDF, ese costosísimo proceso será historia en muy poco tiempo.*

Cada año, el Colegio de Ingenieros de Caminos, Canales y Puertos de España (CICCP) se enfrenta a la tarea almacenar y verificar millones de documentos de gran complejidad (planos de carreteras, puertos, puentes), realizados en cualquiera de las 52 provincias españolas.

Una sola copia de los cientos de planos necesarios para construir nueve kilómetros de ferrocarril ocupa cinco grandes cajones en las dependencias de la institución. Si a otros colegios profesionales los proyectos para visar llegan en pesados y voluminosos paquetes, los relacionados con grandes infraestructuras pueden requerir, incluso, de camiones para su transporte.

De cada proyecto pueden ser necesarios entre cinco y doce copias. Sin contar con que si el proyecto experimenta alguna variación, habrá que repetir el proceso de impresión, ensobrado de planos, encuadernación y envío del original y las copias. Y todavía falta estampar el sello del Colegio en cada página y plano ¡en forma manual!

¿Qué volumen alcanzarán, entonces, una docena de copias de los 5.000 planos requeridos para un proyecto como el de la Línea 9 del Metro de Barcelona? Aunque parezca mentira, apenas un simple CD. La diferencia está en una combinación casi perfecta: la tecnología PKI (en la que se basa la firma digital) con Acrobat PDF.

“No podíamos seguir aplicando tecnologías del Siglo XIX para hacer, presentar y visar los proyectos Siglo XIX”, dice Emilio Marín Barragán, Jefe del Servicio de Informática del Colegio. Es evidente que necesitábamos dar el salto a la firma electrónica”.

Tras varios estudios, el Colegio decidió concretar el proyecto con **ipsCA**, una empresa que emite certificados digitales desde 1995 y que, actualmente es la cuarta autoridad certificadora mundial de certificados ssl X.509 de servidor y la segunda en España de Certificados de usuario.

El proyecto comenzó en febrero de 2003, con la distribución de tarjetas inteligentes y sus correspondientes lectores entre algunos de sus colegiados para la aprobación de los planos mediante la firma digital. La idea era trasladar los documentos en papel al formato digital, gracias al hoy tan popular PDF, Adobe. Así el ingeniero agrega su firma electrónica al archivo y lo envía a la persona encargada de su revisión, que a su vez puede añadir todos los cambios necesarios. De esta forma, las miles de páginas de planos de proyectos complejos se convierten en un par de gigas de información electrónica, lo que permite enviarlo vía email, ftp o CD para su posterior almacenamiento definitivo.

Esta experiencia basada en productos de Adobe e ipsCA, más tarde se trasladó a otros colegios profesionales, entre ellos:

- Colegio de Ingenieros de Caminos, Canales y Puertos
- Colegio Oficial de Ingenieros Industriales de Madrid
- Colegio Oficial de Arquitectos de Madrid
- Colegio Oficial de Ingenieros Industriales de Aragón y La Rioja
- Colegio Oficial de Ingenieros Industriales de Canarias
- Colegio Oficial de Ingenieros Técnicos Industriales de Navarra
- Colexio Oficial de Arquitectos de Galicia
- Colegio Oficial de Aparejadores y Arquitectos Técnicos de Cáceres.

Cómo funciona
El proyecto desarrollado por el CICCP e ipsCA se basa en el producto denominado **U Sign PDF**, que incorpora el formato PDF de Adobe Inc., con el añadido de mejoras como el soporte de certificados digitales X.509 y el sellado de la fecha del documento.

El Colegio proporciona al profesional un carnet digital, dotado con un microchip criptográfico que lo identifica como colegiado; también recibe el software que le permite estampar esa firma en un documento PDF. Posteriormente, y con el mismo método, el Colegio añade el sello de visado, también electrónico.
De este modo, ese PDF se puede enviar a la Administración o destino correspondiente, con la garantía de que tanto la autoría como el registro de visado han sido realizados. El archivo no se puede modificar sin invalidar permanentemente las firmas, tanto del Colegiado autor como de Visado del Colegio".

Sin embargo, más allá de los evidentes beneficios para los involucrados, el Colegio se enfrentaba a un reto difícil: que las administraciones públicas aceptaran los documentos en formato electrónico."Paradójicamente, la legislación española se había adelantado a los hechos, y en muchos casos, había más disposición que medios.

BOX
El caso en cifras
- Colegiados: más de 20 mil
- Documentos verificados y almacenados: más de 20 millones
- Autoridad Certificadora: El propio colegio.
- Expedientes visados al año: 24.000 (promedio)
- Implementación del proyecto: Febrero de 2003 (tras una prueba piloto en 2002 con 300 profesionales) a 2005.
- ROI (sólo en el primer año): €12 millones (sólo en ahorro de costos de impresión y encuadernación).

BOX
Qué es la firma electrónica
La firma electrónica consiste en añadir a cualquier archivo, generado por medios electrónicos, la identificación única de quien es su autor y otras características como fecha, integridad (la seguridad de que no fue modificado), etc. Se trata de un código secreto conocido como **clave privada**, almacenado en la propia tarjeta y que también puede guardarse en el disco duro de la computadora y en otros dispositivos de almacenamiento. El software ActivCard generara un par de códigos: la mencionada clave privada y otra pública. La combinación de ambas (llamada **tecnología PKI** o infraestructura de clave pública) hace matemáticamente imposible revelar el contenido del documento a quien no tenga la llave para su decodificación. Este sistema también facilita la transmisión segura de los documentos desde cualquier computadora en cualquier lugar, ya que sólo la tarjeta y el PIN secreto activan el mecanismo de seguridad.
Las ventajas del sistema van más allá del ahorro: permite reducir los errores. Si un documento electrónico se firma digitalmente en sus múltiples revisiones, se evitarán cambios indeseados producidos de forma accidental o maliciosa por manos no autorizadas. Es por tanto un problema que atañe tanto a la economía como a la seguridad.

Aplicado al visado digital, garantiza la identidad, titulación y habilitación de la persona que suscribe un trabajo, así como la autenticidad, el registro y la corrección de la presentación de los archivos según la normativa.

El sistema permite a los colegiados firmar electrónicamente sus documentos, con igual validez legal que una firma manuscrita, sólo que ahorra tiempo, costos y esfuerzo logístico; disminuye drásticamente el uso de papel, tintas, copias, encuadernación y espacio de almacenamiento. Así cambian las colas, esperas y el transporte de toneladas de proyectos en papel por documentos PDF firmados electrónicamente que pueden enviar en CD o vía email.

Más información
www.ipsca.com
www.ciccp.es
www.fiadi.org **CLAU: OJO QUE YA TE PUSE LA PÁGINA WEB DEL CONGRESO DE FIADI**

€ 1.200 costaba cada uno de los cajones de madera que se tuvieron que construir para transportar los planos de la presentación del proyecto para la ampliación del Aeropuerto de Barajas.

12 días es el ahorro de tiempo que significó el empleo de la firma digital en el proceso de aprobación de bocetos.

Opinión

Los abogados en la era digital

Por Rodolfo Lomascolo, director general de ipsCA

La firma electrónica es un procedimiento mediante el cual se asocia la identidad de una persona a un documento, algo equivalente a una huella electrónica. De esta forma, puede vincularse a un archivo para identificar al autor, para señalar conformidad (o disconformidad) con el contenido, para indicar que ha sido leído o, según el tipo de firma, para garantizar que no pueda modificarse. Su principal cometido es agilizar procesos, ahorrar dinero, garantizar la seguridad de los trámites y convertir cualquier procedimiento habitual en una operación sencilla, cómoda y fiable. Por eso puede resultar de gran utilidad a los abogados de muy diversas formas. Gracias a ella, no sólo queda garantizada la identidad del emisor, sino que el documento firmado electrónicamente goza de plena validez legal.

Estas herramientas se adaptan perfectamente a las peculiaridades del trabajo de los letrados, evitándoles moverse de su oficina para solicitar documentación o para entregarla de forma certificada. Asimismo, todo el proceso de firma de informes, contratos, facturas, aprobaciones, visados o cualquier otro tipo de documento que requiera de validación, se puede automatizar de forma sencilla y con altos volúmenes de trabajo, gracias a herramientas específicas.

Otro punto a tener en cuenta es que la legislación vigente otorga plena validez legal al procedimiento, lo que autoriza a reemplazar sin problemas la documentación en papel. De esta forma, no sólo se obtiene un importante ahorro de tiempo y dinero –con la supresión de gastos de envío, impresión, etc-, sino que también se elimina la necesidad de contar con espacio físico para almacenar los documentos firmados.

CONTACTO DE PRENSA

Muriel Mirvois
aleph.comunicacion@gmail.com
4556-1467 / 15 6106-6560
www.alephcom.es

Medio: Red Users/ Expand IT
Tema: Firma digital para Pymes
Por: *Rodolfo Lomascolo, CEO de* ipsCA y *VP para Iberia y LatAm de* STS Group

---

Versión Final - 3-11-2009

A pesar de que el intercambio de datos e información por medios electrónicos no deja de crecer -tanto en el ámbito individual como en el mundo corporativo- la *e-economía* no acaba de cuajar masivamente y el papel sigue siendo el rey. Tan es así que aún hoy:

- el 96% de los documentos críticos de las empresas circula en papel;
- 90% de la comunicación con los clientes se realiza en soporte físico.
- el 30 al 70% del tiempo de un empleado es dedicado a la gestión de documentos.
- El costo de la gestión de documentos representa del 6 al 15% de los ingresos de una empresa

* Fuente: Gartner Group, Ashburnham Group, Cap Ventures, Coopers & Lybrand, Forrester Research, Ikon Office Solutions, Dataquest

Y esto se debe sobre todo a un problema de confianza: ¿Cómo garantizar que las personas que se mueven en un entorno electrónico son quienes dicen ser? ¿Cómo asegurar la integridad y confidencialidad de los datos y documentos intercambiados y archivados en soporte digital? ¿Cómo establecer un enlace claro entre un documento electrónico o una acción y una persona, demostrable en un entorno jurídico? ¿Cómo estar seguros de que un intercambio o archivo digital es legalmente apto para usarse como prueba?

Por eso, las tecnologías de **firma digital** y certificados digitales están experimentando un claro crecimiento en todo el mundo. España, por ejemplo, se ha convertido en líder mundial, con más de 12 millones de certificados emitidos- y recientemente se dio a conocer que casi la mitad (49%) de las empresas españolas ya está utilizando esta tecnología. En Latinoamérica su adopción es todavía muy lenta, aunque en México, Ecuador, Chile y Costa Rica son los países de la región donde más se está moviendo.

En el caso puntual de Argentina, el nivel de penetración es escaso: a pesar de los casi ocho años trascurridos desde la sanción de la **ley** que le otorgó el mismo status legal que a la firma manuscrita, la firma digital solo se utilizaba en el ámbito de la administración pública. Pero a principios de agosto AFIP dio a conocer una serie de medidas para agilizar y controlar el comercio, entre las que se encuentran el uso de la **firma digital en los contratos de compra-venta de granos**. Aunque hay mucho camino por recorrer, es un avance importante para que las empresas comiencen a incorporar esta herramienta a sus procesos de negocio.

Firma digital y pymes: usos y ventajas

En un enfoque amplio, la firma digital puede aplicarse a empresas o instituciones de cualquier tamaño que requiera la firma manuscrita en sus procesos y a aquellos entornos donde la autenticación o la verificación de la identidad de las partes resulte fundamental:

- Workflows de aprobación internos con varios decisores.
- Firma de contratos con empresas y personas a distancia.
- Presentación de proyectos o documentos que requieren actualización constante y cuya última versión aprobaba debe enviarse a clientes y proveedores.
- Acreditación de identidad: autenticación de usuarios para el acceso a una red y datos y documentos sensibles; seguridad para el correo corporativo; controles de acceso remoto; *single sign on*; tarjetas de acceso, etc.
- Factura electrónica (en los países donde requieren estar firmadas)
- Comercio electrónico.
- Banca electrónica.
- Operaciones de importación/exportación.
- Digitalización y desmaterialización certificada de archivos físicos.
- Receta electrónica / historia clínica digital
- Gestión de RRHH (e-nómina)
- Firma de créditos, microcréditos, hipotecas, pólizas de seguro.
- Factura electrónica (en aquellos países en los que las facturas requieren estar firmadas)
- Receta electrónica / historia clínica digital
- Formularios electrónicos
- Registro y gestión de documentos para ingenieros, arquitectos, abogados, contadores, escribanos, etc.(colegios y concejos profesionales)
- Tasaciones
- Certificados catastrales
- Presentación de Balances y Cuentas

En cuanto a las **ventajas**:

- Refuerza la seguridad de los datos sensibles de la pyme y los de sus clientes mediante un mecanismo sencillo, de fácil instalación, que no requiere una gran infraestructura IT, y sobre todo, **a un costo accesible**: **con una inversión de sólo u$ 60 (el producto más básico) cualquier empresa, particular o institución puede empezar a firmar digitalmente**; todo depende del uso y volumen de documentos o procesos a firmar.
- Modernización y agilización de los procesos de negocio.
- Facilita su incorporación a la cadena de distribución y proveedores de grandes empresas.
- Permite establecer relaciones de confianza en las comunicaciones electrónicas en entornos B2B, B2C, B2P y P2P: para el e-commerce; para el correo corporativo; protección de acceso a datos y documentos sensibles; etc.
- Importantes ahorros de costos (papel, impresión, mano de obra, archivado, logística, subsanación de errores, etc.)
- Ahorro de tiempos / Inmediatez: (el trabajo online permite firmar documento en cualquier sitio con conexión a Internet)
- Retornos de la inversión (ROI) en corto tiempo.
- Control de modificaciones (autenticidad) y reducción de errores (evita cambios indeseados producidos de forma accidental o maliciosa por manos no autorizadas)
- Brinda seguridad, integridad, auditabilidad y trazabilidad a los datos así como a los intercambios y transacciones.
- Permite establecer “evidencias electrónicas” y que los datos sean jurídicamente aceptables (valor probatorio)
- Conservación de las pruebas y evidencias electrónicas a mediano plazo.
- Garantizarla identificación de las personas
- **Es una poderosa arma contra el pishing, el fraude, el robo de identidad y otros delitos digitales.**
- Preserva la confidencialidad.
- Mayor productividad
  –Automatización de revisión y aprobación de documentos
  –Acceso a la información por otras aplicaciones/usuarios
- **Es una forma fiable de controlar la gestión de identidades y privilegios en un entorno SaaS**, para que el acceso a los datos se haga de forma ordenada y segura.

Algunos consejos

Es recomendable que las compañías que se interesen por implementar estos mecanismos tengan en cuenta algunos puntos importantes:

1. Animarse a innovar. La experiencia indica que son las empresas –junto con el estado-las que le dan el impulso decisivo a estas tecnologías incorporándolas a sus procesos de negocio. Si bien la penetración de la firma digital hoy es muy baja, sobre todo porque aún no circulan certificados en el ámbito privado, se puede comenzar implementado sistemas de firma electrónica y poco a poco migrar a la digital.
2. Recuerde que a la larga “lo barato sale caro”: recurra a un proveedor especializado, de experiencia probada, ya que en el mercado abunda la oferta de consultores, integradores, desarrolladores, etc. que “tocan de oído”.
3. Evaluar si la solución o herramienta que le ofrece el proveedor cumple con los estándares internacionales, si se trata de un software auditado, homologado, qué valor probatorio ofrece, etc.
4. Tener presente que los documentos electrónicos (firmados o no firmados digitalmente) a lo largo del tiempo pueden perder algunas propiedades relativas a la seguridad: por debilitamiento de los procesos de securización, por cambios en los estándares requeridos en cada momento, etc. En definitiva, tenga presente obsolescencia tecnológica, que cada vez es más veloz.
5. Pensar en el largo plazo. Analizar exhaustivamente las necesidades de la empresa: si sólo necesita firmar documentos, si requiere enviar notificaciones seguras; si requiere archivar y resguardar toda la cadena de confianza del objeto digital a lo largo de su ciclo de vida; si necesita que sus documentos estén dotados de valor probatorio (que puedan ser aceptados como prueba en un tribunal).
6. Determinar el enfoque más adecuado y rentable. Muchas empresas, bien por su giro, por su infraestructura de TI o por sólo requerir de firma en momentos puntuales, no se inclinan por implementar un entorno complejo de firma y prefieren moverse en un esquema SaaS, en el que pagan únicamente por cada documento que necesiten firmar/archivar.

Muriel Mirvois
Coordinadora de cuentas
Argentina: 4781-9058 / 15 6106-6560
México: 55 8421-8412
muriel@alephcom.com.ar
www.alephcom.es

TEXTO ORIGINAL

A pesar de que el intercambio de datos e información por medios electrónicos no deja de crecer -tanto en el ámbito individual como en el mundo corporativo- la *e-economía* no acaba de cuajar masivamente y el papel sigue siendo el rey. Tan es así que aún hoy:

- el 96% de los documentos críticos de las empresas circula en papel;
- 90% de la comunicación con los clientes se realiza en soporte físico.
- el 30 al 70% del tiempo de un empleado es dedicado a la gestión de documentos.
- El costo de la gestión de documentos representa del 6 al 15% de los ingresos de una empresa

* Fuente: Gartner Group, Ashburnham Group, Cap Ventures, Coopers & Lybrand, Forrester Research, Ikon Office Solutions, Dataquest

Y esto se debe sobre todo a un problema de confianza: ¿Cómo garantizar que las personas que se mueven en un entorno electrónico son quienes dicen ser? ¿Cómo asegurar la integridad y confidencialidad de los datos y documentos intercambiados y archivados en soporte digital? ¿Cómo establecer un enlace claro entre un documento electrónico o una acción y una persona, demostrable en un entorno jurídico? ¿Cómo estar seguros de que un intercambio o archivo digital es legalmente apto para usarse como prueba?
Por eso, las tecnologías de firma digital y certificados digitales están experimentando un claro crecimiento en todo el mundo. España, por ejemplo, se ha convertido en líder mundial, con más de 12 millones de certificados emitidos- y recientemente se dio a conocer que casi la mitad (49%) de las empresas españolas ya está utilizando esta tecnología. En Latinoamérica su adopción es todavía muy lenta, aunque en México, Ecuador, Chile y Costa Rica son los países de la región donde más se está moviendo.
En el caso puntual de Argentina, el nivel de penetración es escaso: a pesar de los casi ocho años trascurridos desde la sanción de la ley que le otorgó el mismo status legal que a la firma manuscrita, la firma digital solo se utilizaba en el ámbito de la administración pública. Pero a principios de agosto AFIP dio a conocer una serie de medidas para agilizar y controlar el comercio, entre las que se encuentran el uso de la **firma digital en los contratos de compra-venta de granos**. Aunque hay mucho camino por recorrer, es un avance importante para que las empresas comiencen a incorporar esta herramienta a sus procesos de negocio.

NOTA: SI POR RAZONES DE ESPACIO, ES NECESARIO ACORTAR EL TEXTO, LOS DOS APARTADOS SIGUIENTES (en qué consiste la FD y diferencias con la firma electrónica) PUEDEN REEMPLAZARSE POR ESTE LINK en cualquier parte del párrafo anterior donde se mencione "firma digital".
http://www.pki.gov.ar/index.php?option=com_content&view=article&id=91&Itemid=102

¿En qué consiste la *firma digital*?
Su objetivo básico es aportar a los documentos electrónicos la misma funcionalidad que la firma manuscrita otorga a un documento impreso: identificar al autor (en Argentina, adquirió la misma validez legal que la firma manuscrita gracias a la Ley 25.506, sancionada en 2001).
Contrario a lo que muchos suponen, la firma digital no es una representación gráfica de una firma manuscrita. Se trata de un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje. En concreto, es un archivo informático que, mediante complejísimos algoritmos, identifica al firmante a través de un par de códigos únicos (llamados *clave privada* y *clave pública*), cuya característica es que la información cifrada con uno de ellos sólo puede ser descifrada con el otro.
Mediante una función matemática, el firmante genera una *huella digital* propia del mensaje, la cual se cifra con la clave privada. El resultado es lo que se denomina *firma digital*, y puede adosarse a cualquier tipo de documento electrónico (texto, audio, foto, video, formularios, etc.), junto con otros datos como la fecha, si fue modificado después de la firma, etc.
A su vez, la *firma digital* se genera a partir de un *certificado (*emitido por una *autoridad cetificadora* licenciada por el ente de aplicación, en este caso, la ONTI*)*, que prueba la vinculación entre una clave pública y un individuo o entidad, lo que ayuda a prevenir que alguien utilice una clave para hacerse pasar por otra persona.
El mecanismo permite que tanto el emisor como el receptor de un documento electrónico se identifiquen mutuamente y tengan la plena certeza de que su contraparte es quien dice ser, evitando que terceros intercepten los contenidos, los alteren o suplanten la identidad. En síntesis, proporciona –tanto a empresas como a ciudadanos- garantías jurídicas para la realización de transacciones y gestiones seguras por medios electrónicos.

¿Firma digital o firma electrónica?
Para la legislación argentina los términos *firma digital* y *firma electrónica* no tienen el mismo significado. Pero contrario a una creencia bastante extendida, ambas tienen validez legal. La diferencia radica en el valor probatorio: si un documento firmado digitalmente es verificado correctamente, se presume **salvo prueba en**

contrario, que proviene del suscriptor del certificado asociado y que no fue modificado. **En el caso de la *firma electrónica*, se invierte la carga de la prueba**: de ser desconocida por su titular, corresponde a quien la invoca acreditar su validez. En el aspecto técnico, para firmar *digitalmente* se necesita un certificado, que acredita la titularidad de la firma (es como el DNI de la firma electrónica) y que se incluye en el documento electrónico a través de un software de firma digital. La *firma electrónica* se realiza mediante un software diferente, y no incluye ningún elemento que asegure la integridad del documento, la identidad, etc.

Firma digital y pymes: usos y ventajas

En un enfoque amplio, la firma digital puede aplicarse a empresas o instituciones de cualquier tamaño que requiera la firma manuscrita en sus procesos y a aquellos entornos donde la autenticación o la verificación de la identidad de las partes resulte fundamental:

- Workflows de aprobación internos con varios decisores.
- Firma de contratos con empresas y personas a distancia.
- Presentación de proyectos o documentos que requieren actualización constante y cuya última versión aprobaba debe enviarse a clientes y proveedores.
- Acreditación de identidad: autenticación de usuarios para el acceso a una red y datos y documentos sensibles; seguridad para el correo corporativo; controles de acceso remoto; *single sign on*; tarjetas de acceso, etc.
- Factura electrónica (en los países donde requieren estar firmadas)
- Comercio electrónico.
- Banca electrónica.
- Operaciones de importación/exportación.
- Digitalización y desmaterialización certificada de archivos físicos.
- Receta electrónica / historia clínica digital
- Gestión de RRHH (e-nómina)
- Firma de créditos, microcréditos, hipotecas, pólizas de seguro.
- Factura electrónica (en aquellos países en los que las facturas requieren estar firmadas)
- Receta electrónica / historia clínica digital
- Formularios electrónicos
- Registro y gestión de documentos para ingenieros, arquitectos, abogados, contadores, escribanos, etc.(colegios y concejos profesionales)
- Tasaciones
- Certificados catastrales
- Presentación de Balances y Cuentas

En cuanto a las **ventajas**:

- Refuerza la seguridad de los datos sensibles de la pyme y los de sus clientes mediante un mecanismo sencillo, de fácil instalación, que no requiere una gran infraestructura IT, y sobre todo, **a un costo accesible**: **con una inversión de sólo u$ 60 (el producto más básico) cualquier empresa, particular o institución puede empezar a firmar digitalmente**; todo depende del uso y volumen de documentos o procesos a firmar.
- Modernización y agilización de los procesos de negocio.
- Facilita su incorporación a la cadena de distribución y proveedores de grandes empresas.
- Permite establecer relaciones de confianza en las comunicaciones electrónicas en entornos B2B, B2C, B2P y P2P: para el e-commerce; para el correo corporativo; protección de acceso a datos y documentos sensibles; etc.
- Importantes ahorros de costos (papel, impresión, mano de obra, archivado, logística, subsanación de errores, etc.)
- Ahorro de tiempos / Inmediatez: (el trabajo online permite firmar documento en cualquier sitio con conexión a Internet)
- Retornos de la inversión (ROI) en corto tiempo.
- Control de modificaciones (autenticidad) y reducción de errores (evita cambios indeseados producidos de forma accidental o maliciosa por manos no autorizadas)
- Brinda seguridad, integridad, auditabilidad y trazabilidad a los datos así como a los intercambios y transacciones.
- Permite establecer “evidencias electrónicas” y que los datos sean jurídicamente aceptables (valor probatorio)
- Conservación de las pruebas y evidencias electrónicas a mediano plazo.
- Garantizarla identificación de las personas
- **Es una poderosa arma contra el pishing, el fraude, el robo de identidad y otros delitos digitales.**
- Preserva la confidencialidad.
- Mayor productividad
  –Automatización de revisión y aprobación de documentos

–Acceso a la información por otras aplicaciones/usuarios

- **Es una forma fiable de controlar la gestión de identidades y privilegios en un entorno SaaS**, para que el acceso a los datos se haga de forma ordenada y segura.

Algunos consejos

Es recomendable que las compañías que se interesen por implementar estos mecanismos tengan en cuenta algunos puntos importantes:

7. Animarse a innovar. La experiencia indica que son las empresas –junto con el estado-las que le dan el impulso decisivo a estas tecnologías incorporándolas a sus procesos de negocio. Si bien la penetración de la firma digital hoy es muy baja, sobre todo porque aún no circulan certificados en el ámbito privado, se puede comenzar implementado sistemas de firma electrónica y poco a poco migrar a la digital.
8. Recuerde que a la larga “lo barato sale caro”: recurra a un proveedor especializado, de experiencia probada, ya que en el mercado abunda la oferta de consultores, integradores, desarrolladores, etc. que “tocan de oído”.
9. Evaluar si la solución o herramienta que le ofrece el proveedor cumple con los estándares internacionales, si se trata de un software auditado, homologado, qué valor probatorio ofrece, etc.
10. Tener presente que los documentos electrónicos (firmados o no firmados digitalmente) a lo largo del tiempo pueden perder algunas propiedades relativas a la seguridad: por debilitamiento de los procesos de securización, por cambios en los estándares requeridos en cada momento, etc. En definitiva, tenga presente obsolescencia tecnológica, que cada vez es más veloz.
11. Pensar en el largo plazo. Analizar exhaustivamente las necesidades de la empresa: si sólo necesita firmar documentos, si requiere enviar notificaciones seguras; si requiere archivar y resguardar toda la cadena de confianza del objeto digital a lo largo de su ciclo de vida; si necesita que sus documentos estén dotados de valor probatorio (que puedan ser aceptados como prueba en un tribunal).
12. Determinar el enfoque más adecuado y rentable. Muchas empresas, bien por su giro, por su infraestructura de TI o por sólo requerir de firma en momentos puntuales, no se inclinan por implementar un entorno complejo de firma y prefieren moverse en un esquema SaaS, en el que pagan únicamente por cada documento que necesiten firmar/archivar.

Medio: CXO Community
Edición: Mayo 09
Tema: Identidad Digital
Tipo de nota: artículo explicativo+ columna de opinión
Foto: DNI Electrónico español.
Epígrafe
Más de 6,5 millones de españoles ya disponen del nuevo DNI electrónico, que comenzó a entregarse en marzo de2006 y ha logrado una penetración que superó todas las previsiones.
Destacados
"El gran punto a favor del DNI electrónico es las posibilidades de uso que todavía están por explotar. En un futuro no muy lejano comenzaremos a ser partícipes de la incorporación de la identidad digital a todos los procesos de negocio. Su desarrollo traerá beneficios económicos al individuo y a las empresas, al facilitar las transacciones mercantiles y personales (e-commerce, gobierno y administración electrónicas, entre otras.**"**
"Convertir la tecnología en invisible y transparente a los ojos del usuario es la mejor manera de hacer prosperar los negocios.**"**

Título: **Identidad digital: Los retos de su gestión**
Bajada: ***El concepto responde a la necesidad de otorgar identificación personal segura a los ciudadanos en la nueva Sociedad de la Información, además de servir como su impulsor. El e-DNI es una de las patas en las que se asienta la identidad digital, junto con la factura electrónica y el e-commerce, y no son otra cosa que la adaptación del tradicional documento de identidad a la nueva realidad de una sociedad globalizada e interconectada por redes digitales de comunicación.***
Por *Rodolfo Lomascolo, director general de* ipsCA*

Por definición, identidad es aquel conjunto de rasgos propios de un individuo que lo caracterizan frente a los demás. Su verificación es lo que nos permite determinar que un sujeto es quien dice ser. Algunos de estos rasgos son propios del individuo; otros son adquiridos con el tiempo. Por supuesto, no todos son igualmente apreciables. Algunos son identificables a simple vista, mientras que otros están ocultos y es necesario un conocimiento y, en ocasiones, herramientas para verificarlos. Al conjunto de rasgos que caracterizan a un individuo en el mundo digital se lo conoce como **Identidad Digital.**

En cualquier comunicación remota, el número de rasgos visibles al que tenemos acceso disminuye. En el universo de Internet, los rasgos -representados por datos en forma de bytes- son procesados por las aplicaciones correspondientes y presentados en el formato requerido. Cada una de las partes de ese intercambio debe confiar en los procesos que llevan a la generación, transmisión y presentación de los datos. La identidad digital no existe a priori: debemos crearla y vincularla unívocamente al individuo, en un proceso que determinará el nivel de confianza en el sistema.

Los retos
Desde la década de los 90, la evolución de las TI en todo el planeta ha sido aún mayor de lo que se podía prever; desde ordenadores personales omnipresentes en casi todos los campos económicos - convertidos incluso en un electrodoméstico a la altura de la televisión-, hasta pequeños chips electrónicos incorporados a una enorme diversidad de dispositivos: desde automóviles hasta el DNI. Así hoy comienza a hacerse imprescindible acreditar la identidad en el nuevo mundo virtual, en las más diversas transacciones electrónicas que se pueda imaginar, con las mismas garantías que en el mundo real.

La posibilidad de firma electrónica utilizando este nuevo DNI será lo que tendrá mayor impacto. La firma, es decir, la representación de la identidad de una persona, ya no dependerá de su presencia física o de una representación gráfica (como ocurre con la manuscrita). La firma electrónica se podrá utilizar en cualquier operación telemática que se adapte para este fin y si se generaliza su utilización dará muchas posibilidades al comercio electrónico y a cualquier tipo de operación que requiera firma.

Precisamente, Internet ha propiciado el auge del **comercio electrónico**, que año tras año no para de crecer y ha traído de su mano la consolidación de la identidad digital. Habiendo dinero involucrado en las transacciones, se hacen aún más necesarios sistemas y herramientas que garanticen la confianza y la seguridad en las operaciones online, tanto para el emisor como para el receptor. Así, la **firma electrónica, los certificados digitales, los dispositivos biométricos, las smart cards o los one-time passwords** se han convertido en mecanismos cada vez más habituales.

¿Qué es el DNI electrónico?

Lejos del tristemente célebre intento que se hizo en los 90 por modernizar la emisión del Documento Nacional de Identidad en nuestro país –salpicado por un escándalo de coimas ue aún hoy continúa en investigación-, el DNI electrónico es mucho más que un carnet con una foto y firma digitalizadas.
La seguridad y la privacidad son los ejes básicos de este dispositivo, y para ello se incluye un chip con toda la información en formato digital y varios certificados, uno para autenticar la identidad del ciudadano y otro para la firma electrónica. Los datos incluidos en formato electrónico dependerán de cada país o región, pero puede contener: huella digital, fotografía del propietario, la propia imagen de su firma y la información que ya constaba impresa en el documento impreso.

Asimismo, permite incorporar técnicas biométricas de reconocimiento, que refuerzan la seguridad y confidencialidad del propietario, ya que todos los accesos a los datos personales quedan puntualmente registrados, pudiendo ser consultados en forma exclusiva por el titular.

Entre las principales ventajas que ofrece -tanto al mundo empresarial como para el ciudadano- destacan: su mayor seguridad, la posibilidad de identificarse en el mundo virtual de forma fidedigna (a través de la firma electrónica) y la simplificación de engorrosos trámites hasta ahora habituales, como el pago de impuestos o la solicitud de documentación.

Pero el gran punto a favor del DNI electrónico es las posibilidades de uso que todavía están por explotar. En un futuro no muy lejano comenzaremos a ser partícipes de la incorporación de la identidad digital a todos los procesos de negocio: la utilización de aplicaciones certificadas, la firma electrónica de documentos mediante teléfonos móviles y PDAs con tan sólo insertar un carnet o el acceso a servicios bancarios multimedia. La firma de contratos de forma telemática y con plena validez legal, el voto electrónico, la identificación en cuentas de correo, la comprobación de la edad en el caso de comprar tabaco en una expendedora automática o incluso la asistencia y ejercicio del voto en juntas de accionistas y consejos de administración de forma remota son ya igualmente factibles. Las posibilidades de la identidad digital son inmensas.

Con el nuevo dispositivo, que permite utilizar la Firma Electrónica, se mejorará la eficiencia de los servicios de la Administración, se potenciará la contratación electrónica, el acceso a recursos on-line será más seguro y se reforzará la participación pública en los procesos de decisión. Asimismo, se eliminará el 80% de certificaciones en papel, permitirá al ciudadano identificarse sin dudas y firmar documentos electrónicos con la misma validez jurídica que los manuscritos. En cuanto a las empresas, les aportará capacidad de innovación una nueva forma de comunicarse con sus clientes, surgiendo así nuevas oportunidades de negocio. El impacto del DNI electrónico como de la Firma Electrónica en el comercio será enorme.
Las empresas, por su parte, podrán agilizar la firma de contratos entre sí y con sus clientes y proveedores, obteniendo un plus en materia de cobertura legal para cualquier operación validada mediante este método.

La tercera pata
Además de la identificación digital y el e-commerce, la **factura electrónica** completa el triángulo en el que se apoya la identidad digital. Cada vez son más las empresas que optan por la facturación electrónica, otro auténtico reto que no sólo permite el ahorro de costos: es respetuoso con el medioambiente y facilita los trámites, la gestión documental y el almacenamiento más eficaz que conlleva la eliminación del espacio físico. Reemplazarlos por formatos más robustos y ágiles, es beneficiosa para el emisor y toda una garantía de seguridad para ambas partes.

ipsCA, como compañía especializada en certificación digital y firma electrónica, ha sido una de las principales impulsoras de la consolidación de la identidad digital en España, apostando por lo que hoy es ya una realidad cotidiana en casi todas las grandes empresas, y en menor medida –aunque creciendo exponencialmente, en la pyme y entre los profesionales autónomos. Desde ipsCA estamos convencidos de que su desarrollo traerá beneficios económicos tanto al individuo como al colectivo, al facilitar las transacciones mercantiles y personales (como el comercio electrónico, entre muchas otras). Y seguiremos trabajando para que todo tipo de usuarios puedan preocuparse exclusivamente por qué quieren o necesitan hacer, y nunca por cómo. Convertir la tecnología en invisible y transparente a los ojos del usuario es la mejor manera de hacer prosperar los negocios. Y a la hora de ver los resultados se acaba notando.

El caso español
El DNI electrónico es ya una realidad en España. Después de distintas fases de prueba e implantación desde 2000, comenzó a expedirse gradualmente desde marzo de 2006, y en la actualidad todo nuevo trámite remite al formato digital.

- El nuevo carnet, de tamaño y color similares al tradicional, se entrega prácticamente en el mismo momento de su petición en la oficina de expedición del DNI de la policía de cada demarcación.
- Incluye un chip criptográfico en su anverso con toda la información en formato digital y varios certificados, uno para autenticar la identidad del ciudadano y otro para la firma electrónica. Entre la información incluida en formato electrónico se encuentra: la huella digital, la fotografía del propietario, la propia imagen de su firma y la información que ya constaba impresa en el propio DNI, un certificado cualificado para

autenticación y otro para firma, certificado electrónico de la autoridad emisora y el par de claves (pública y privada) de cada certificado electrónico. No contiene información relativa a datos personales distintos a los que aparecen impresos en la superficie de la tarjeta ni información sanitaria, fiscal, judicial, penal, infracciones de tráfico, etc.

- Tecnológicamente, cuenta con tres niveles de seguridad: en el primer nivel, holograma, letras táctiles, imágenes láser cambiantes; en un segundo nivel, imágenes codificadas, microtextos, kinegramas; y, por último, medidas criptográficas y biométricas.
- Se espera que la utilización de este nuevo formato producirá un importante auge de la autenticación online, materializado principalmente en un despegue del *e-commerce* así como en la agilización de la relación de los ciudadanos con **la Administración Pública, que es precisamente la que está encabezando la mayoría de las iniciativas.**
- **En números,** la penetración del e-DNI ha superando las previsiones más optimistas.
    - Más de 6,5 millones de españoles disponen del nuevo documento, con lo que su popularización se prevé masiva en apenas unos meses.
    - Más de 300 puntos de expedición (dependientes del Cuerpo Nacional de Policía).
    - Reducción del trámite a una sola visita, y no en dos como sucedía con anterioridad.
    - Más de 400 servicios prestados actualmente en formato telemático por la Administración Pública, con seguridad, desde la comodidad del hogar y a cualquier hora, sin ventanillas ni colas.
    - Además, Ya no es necesario aportar la documentación que se pueda remitir electrónicamente desde el órgano administrativo en que se ésta se encuentre a la Dirección General de la Policía, con lo que el papeleo y los trámites se ven agilizados notablemente.

RECUADRO
CASOS DE ÉXITO

- **IpsCA** ha desarrollado todo el sistema de identificación de los ciudadanos de Andorra (equivalente al DNI electrónico). En el proyecto se ha implantado el Sistema de Cifrado y Firma Digital basado en certificados emitidos por el Gobierno de Andorra y W2000 sobre varios soportes. También se han utilizado sistemas de SSO, Autenticación de Usuarios y Sistemas de Acceso Remoto.
- La **Banca Privada d'Andorra** (BPA) ha puesto en funcionamiento un sistema de tokens desarrollado por **ipsCA** conjuntamente con Actividentity, basado en contraseñas de un solo uso, para blindar y agilizar las transacciones on-line. El sistema protege a los clientes de problemas como el ***phishing*** (robo de datos y suplantación de identidad), el ***pharming*** (desvío a webs falsas)
    - Después de pulsar el único botón que tiene el MiniToken se genera la clave de un solo uso que el cliente introduce en a página de entrada del servidor al que quiere acceder, el sistema valida la clave y si es correcta le permite el acceso. El usuario puede realizar esta operación desde cualquier computadora, ya que el sistema no requiere instalación de software. L
    - La eficacia de su funcionamiento se debe a que incorpora internamente algoritmos de máxima seguridad y un temporizador sincronizado con los servidores a los que accede el usuario.
    - Entre las principales ventajas del dispositivo también destacan un importante ahorro de tiempo y dinero (la utilización de contraseñas estáticas o fijas requiere una continua renovación de medidas de seguridad para evitar que alguien capture los datos. Los passwords dinámicos, al ser irrepetibles, eliminan estos gastos.
    - Adicionalmente, el sistema podrá utilizar en banca telefónica, banca presencial -cuando el usuario no dispone de un documento que lo identifique pero dispone del token- o incluso en acceso a sistemas desde puestos de trabajo combinándose con soluciones de Single Sign On.
- **El banco Kas Bank**, una de las entidades bancarias más importantes y con más tradición de Holanda, cuenta desde ¿????? (INDICAR MES Y AÑO) con una **Autoridad Certificadora (CA**) firmada por **ipsCA**, que estará encadenada a la Autoridad Certificadora raíz de la compañía. Así, la entidad bancaria podrá emitir certificados digitales respaldados por la experiencia de ipsCA.
    - Con esta autoridad certificadora –llamada corporativa-, Kas Bank podrá generar cualquier tipo de certificado, ya sean Certificados Personales, de Servidor, para WAP, para firmar Código e incluso para IPSec-VPN, convirtiéndose así en un eficaz sistema de generación de certificados para sus usuarios, desde trabajadores a proveedores o clientes.
    - Así, cuando se opera en la banca online, en lugar de introducir un pin el usuario, firma con su propio certificado electrónico.
- **Otros clientes:** Como Autoridad Certificadora dentro de un entorno PKI, ipsCA emite certificados digitales que sirven para verificar la identidad en la Red. Entre los principales certificados de servidor que proporciona a clientes en todo el mundo destacan muchas de las universidades y centros educativos más relevantes de los Estados Unidos, así como cerca de una veintena de colegios profesionales de España, que cuentan con el sistema de visado digital para recibir y aprobar los proyectos de sus colegiados.

***Ips Certification Authority (ipsCA)** es líder en la fabricación de herramientas de Firma y Facturación Electrónica, y pionera en Europa como Autoridad Certificadora. Con más de doce años de experiencia y 8 mil clientes en el mundo, cuenta con soluciones de firma y facturación electrónica; certificación y visado digital; identidad digital; formularios telemáticos; voto y compulsa electrónica. Ofrece herramientas de escritorio, aplicaciones para servidores y appliance plug&play, tanto para pequeños como grandes volúmenes de documentos, tanto para grandes como pequeñas y medianas empresas, así como particulares y profesionales. Mantiene acuerdos con más de 350 socios y partners, entre los que destacan Adobe, Microsoft –ipsCA es Autoridad Certificadora Raíz para todos su productos, Sun Microsystems, IBM, Safenet, ActivIdentity, HP, Nokia, Lotus y Xerox. **Más información: www.ipsca.com**

CONTACTO DE PRENSA
Muriel Mirvois
4781-9058 / 15 6106-6560
muriel@alephcom.com.ar
Marcela Casarino
15 6193-2310
marcela@alephcom.com.ar

Cómo reducir gastos sin comprometer la seguridad

Por Rodolfo Lomascolo, CEO de ipsCA y VP para Iberia - LatAm de STS Group

Ya no es una novedad para nadie involucrado con las TI que un ataque informático puede tener consecuencias de distinta gravedad para la organización. Y si se tiene en cuenta que la actividad de la Industria del malware y los delitos digitales continúa creciendo cada día, es difícil situarse en un escenario más peligroso. La lista de "amenazas" es larga y va desde el robo o suplantación de identidad hasta el fraude financiero, pasando por el robo o difusión de información sensible o confidencial. Sólo por mencionar un ejemplo difundido recientemente: los proyectos financieros de Twitter aparecieron publicados en un importante medio gracias a que un hacker vulneró una clave demasiado débil y así tuvo acceso al correo electrónico de uno de los ejecutivos de la empresa.

No obstante, ante la difícil coyuntura que atraviesa la economía mundial, muchas empresas se ven obligadas a reducir costos y según un reciente estudio de Deloitte, 32% ha optado por recortar el presupuesto en seguridad TI. Pero las empresas, tanto en tiempos de bonanza como de recesión, requieren soluciones que achiquen sus gastos, pero nunca sus prestaciones. En consecuencia, antes de reducir la partida de seguridad, es necesario plantearse si existen otras alternativas para ahorrar.

El Software como Servicio (SaaS, por sus siglas en inglés) y "la nube", hoy tan en boga, se presentan como otro camino para recortar gastos, así como la posibilidad para las PYMES de acceder a aplicaciones robustas o world class a costos razonables. Lo mismo para compañías que por su naturaleza no están interesadas en montar una infraestructura de TI.

Y si bien el potencial de este modelo ya estaban dando de qué hablar antes de que estallara la tormenta financiera, según las grandes consultoras como Gartner e IDC, será de aquí a los próximos tres años cuando se producirá un crecimiento exponencial en su adopción, hasta convertirse en referencia del mercado, frente al tradicional enfoque de pago por licencias y cliente-servidor.

En el modelo SaaS *o* de "pago por uso" el usuario accede a servicios y aplicaciones a través de Internet, con lo que elimina la necesidad de adquirir licencias, gestionar la infraestructura y preocuparse por el mantenimiento y actualización. Esto implica rápida adopción, costes iniciales reducidos, actualizaciones sencillas; integración perfecta en la infraestructura TI de la empresa, mayor ROI, fácil distribución, portabilidad y escalabilidad (los usuarios pueden estar distribuidos en sitios remotos y acceder en cualquier momento al sistema tan sólo con una conexión a Internet). En definitiva, permite a la empresa enfocarse en sus objetivos de negocio y no en manejar sistemas.

Sin embargo, a pesar de sus múltiples ventajas, muchas organizaciones se muestran renuentes a implementar esta modalidad porque consideran riesgoso delegar el control y administración de su información y datos sensibles a terceros. Y la preocupación no es infundada: toda esta arquitectura multiusuario requieren prestar especial atención a la seguridad, tanta o más que la que se dedica a los sistemas internos.

En este contexto, la firma y los certificados digitales ofrecen un enorme potencial, como el complemento perfecto para controlar y gestionar identidades y privilegios, garantizando la seguridad y confidencialidad. Y si antes dependían de cada terminal físico y lo que se almacenaba en él o en el servidor de la empresa, ahora todo puede estar en la famosa "nube".

La firma digital en formato SaaS es ideal para empresas que, bien por su infraestructura o por requerir esta tecnología sólo en momentos puntuales, no se inclinan por implementar un sistema de este tipo. Ahora, contratándolo en modalidad de software como servicio, pueden pagar únicamente por cada documento que necesiten firmar digitalmente, o como soporte de seguridad para otras aplicaciones.

Tanto en Europa occidental como en EEUU, el mercado muestra una clara tendencia en esa dirección, mientras que en Latinoamérica y los países del este todavía se mueven en el enfoque tradicional.

En el caso puntual de Argentina, es llamativo el bajo nivel de penetración que ha alcanzado la tecnología de firma digital, a pesar de los casi ocho años trascurridos desde la sanción de la Ley 25.506 -que le otorgó el mismo status legal que a la firma manuscrita- y a dos de establecido el marco normativo aplicable al otorgamiento y revocación de licencias para emitir certificados digitales (Decisión Administrativa Nº 6/07).

Lo cierto es que hasta hoy, AFIP y ANSES son los únicos organismos autorizados por la Oficina Nacional de Tecnologías de Información (ONTI) para emitir certificados, mientras que no existe todavía ninguna entidad

privada licenciada. Hasta hace apenas unos días, dichos certificados solamente se utilizaban en el ámbito de la administración pública. Pero a principios de agosto AFIP dio a conocer una serie de medidas para agilizar y controlar el comercio, entre las que se encuentran el uso de la firma digital en los contratos de compra-venta de granos. Según subrayó el titular del organismo, Ricardo Echegaray "será el primer contrato con firma digital entre privados". Para eso, la entidad aprobó la resolución 2651 mediante la cual establece el procedimiento para la emisión de certificados a los contribuyentes. Se trata sin duda de un avance importante y cabe esperar que poco a poco las empresas comiencen a incorporar esta herramienta a sus procesos de negocio. Pero será una transición lenta.

Por su parte, las principales cámaras del sector TI han llamado la atención sobre la eficacia de la firma digital. En documento "Bases y lineamientos para una Agenda Digital Argentina" expresa en el capítulo dedicado al marco jurídico que "El adecuado desarrollo de la nueva economía y del gobierno electrónico requieren de una nueva forma de interactuar entre las personas privadas, entre éstas y la administración pública, reconociéndose la validez y valor probatorio al documento digital y autorizándose el uso de mecanismos de autenticación que puedan utilizarse en dicho ambiente (entre otros, la firma digital) -por lo menos- en las mismas condiciones de validez que posee el formato papel". Y continúa: "(…) podemos afirmar que, si bien se ha avanzado en la materia, existen aplicaciones que utilizan métodos alternativos de autenticación en forma exitosa y que están siendo utilizadas masivamente sin generar repudio de transacciones". El documento cita como ejemplo el sistema de declaraciones juradas de la AFIP, como una de las aplicaciones que utilizan autenticación sin firma digital. Pero no es la única.

En ese sentido, vale la pena mencionar que hay una gran confusión sobre que la firma electrónica (para lo que no se requiere un certificado asociado) tiene menos validez que la digital, una imprecisión que ha retrasado el despegue de estas tecnologías. La realidad es que ambas tienen valor legal. La diferencia radica en el valor probatorio de cada una: en el caso de la firma digital existe una presunción "iuris tantum" en su favor; esto significa que se presume salvo prueba en contrario por parte del demandante que proviene del suscriptor del certificado asociado. En la firma electrónica se invierte la carga probatoria: en caso de ser desconocida la firma, corresponde a quien invoca su autenticidad acreditar su validez. Por ejemplo, si dos partes que celebran un contrato firmado digitalmente una de ellas alegara la invalidez de alguna de las firmas, le corresponde a ésta demostrarlo ante la ley. Si en cambio, las partes firmasen el contrato con firma electrónica, corresponde a la parte que clama por su validez demostrar ante la ley la autenticidad y sólo en caso de no poder demostrarla, esa firma electrónica no es válida.

Nuestra experiencia en Europa indica que el factor determinante para el despegue de la firma digital fue que las empresas comenzaron incorporando la firma electrónica y poco a poco fueron migrando a la digital. Y prácticamente no se conocen casos de repudio que haya llegado a un tribunal.

Estamos en un punto en el que el mercado TI, es más competitivo, en calidad, seguridad y reducción de costes y tiempo. Al juntar estas vertientes encontramos en el modelo SaaS y su aplicación para la e-firma una solución viable para que las empresas le den un valor añadido a sus servicios.

Acerca de ipsCA

Ips Certification Authority (ipsCA) es líder en la fabricación de herramientas de firma y facturación electrónica, además de pionera en Europa como Autoridad Certificadora. En abril de 2009 pasó a formar parte del grupo francés STS, integrando el intercambio y archivo de documentos electrónicos con valor probatorio a su amplia gama de soluciones, entre las que destacan la firma y facturación electrónica; certificación y visado digital, identidad digital, formularios telemáticos; voto y compulsa electrónica. Las herramientas de ***ipsCA*** *destacan por su optimizado diseño, rápida implementación, y compatibilidad con sistemas de identidad digital y DNI electrónico. En la actualidad la compañía dispone de productos de escritorio, aplicaciones para servidores y appliance plug & play que, basados en arquitectura SOA, aúnan toda la propuesta tecnológica de firma electrónica desarrollada por la empresa hasta la fecha.* ***IpsCA*** *mantiene acuerdos con más de 350 socios y partners internacionales, como Adobe, Microsoft –ipsCA es Autoridad Certificadora Raíz para todos los productos de la firma americana–, Sun Microsystems, IBM, Safenet, ActivIdentity, HP, Indra y Xerox, entre otros.*

Acerca de Grupo STS

Grupo STS *nace en el año 2000 como empresa fabricante de software. Sus oficinas centrales están localizadas en Rueil Malmaison (París) y Nîmes. Líder europeo en el intercambio y archivo electrónico con valor probatorio, la compañía está instalada también en España, Italia y Bélgica.Grupo STS cotiza en la Bolsa de Paris y en el Mercado Libre EURONEXT desde noviembre de 2005. Las soluciones de STS aportan un gran valor añadido y han ayudado a más de 250 clientes a adaptarse a las nuevas exigencias del mundo electrónico.*

LAS SOLUCIONES Y HERRAMIENTAS DE ipsCA-STS Group ESTÁN DISPONIBLES EN ARGENTINA A TRAVÉS DE SYSASAP.

CONTACTO DE PRENSA

aleph comunicación

Muriel Mirvois
muriel@alephcom.com.ar

Marcela Casarino
marcela@alephcom.com.ar

Bs. As.: +5411 4781-9058
México: 55 8421-8412

Enmascaramiento de datos: confidencialidad garantizada

Por Alberto Collado, Director General
de PowerData para América Latina
www.powerdataam.com

Desde hace varios años, ha aumentado la preocupación de los gobiernos por proteger la privacidad de los datos. Existen leyes específicas y las penas por su incumplimiento son cada vez más severas. Por eso, las empresas comienzan a tomar **recaudos,** estableciendo estándares de privacidad en todas las áreas de negocio.

La exposición de la información sensible en las organizaciones es un hecho frecuente debido al crecimiento del volumen de la información y a la intensa recolección, uso y tratamiento y almacenamiento de ésta. Los datos confidenciales también corren peligro cuando cruzan fronteras, se produce un uso ilegítimo a través de Internet, o cuando personas no autorizadas acceden a las aplicaciones corporativas (CRM, ERP, etc.). Así, los datos quedan expuestos frecuentemente al robo, la manipulación y la utilización de esa información –muchas veces estratégica- por parte de la competencia. Sin embargo, la mayoría de las veces, el enemigo está en casa: el 70% de las vulnerabilidades de datos ocurre dentro de la organización.

En general, las empresas cumplen con las normativas de protección de datos en sus entornos productivos, con la instalación de armarios ignífugos, controles de acceso, copias de seguridad, encriptación... Sin embargo**,** existen otras "puertas de entrada", como los entornos de formación, desarrollo y pruebas, que muchas veces no cuentan con las mismas medidas de seguridad y los controles de calidad óptimos, en general para abaratar costos. Sin embargo, esos procesos "menos cuidados" están sujetos a las mismas normativas y, además, suelen ser más vulnerables que los entornos de producción.

Los ambientes de pruebas (para el desarrollo de software o proyectos de Business Intelligence, por ejemplo) con frecuencia utilizan copias exactas de los datos reales, ya que resulta muy útil disponer de un gran volumen de información para testear el rendimiento o la respuesta del sistema. Cuando en entornos como estos, no se protegen los datos sensibles**,** se corre el riesgo de un daño irreparable para la imagen de marca (de cara a los inversores, clientes y/ ciudadanos), una repercusión negativa en los medios, una pérdida de clientes y un costo añadido en auditorías.

Por otro lado, las organizaciones suelen establecer diferentes medidas de seguridad para los datos en función de su contenido. Un fichero que contenga sólo nombre, dirección y teléfono requerirá un nivel de seguridad básico, mientras que ciertos datos sensibles –como orientación política o sexual) requerirán un nivel de acceso alto, que incluye medidas de seguridad más estrictas (cifrado de las telecomunicaciones, registro de accesos, entre otras).

En general, las empresas evitan recabar estos datos "conflictivos" para mantener un nivel básico de seguridad y eliminar gastos adicionales. Pero **una inocente anotación de un operador de call center** ("*el cliente no quiere participar en el sorteo porque le acaban de operar de un cáncer*", por ejemplo) **puede transformar automáticamente la base de datos, y sin que nadie lo perciba: ahora contendrá registros que en un principio se habían querido evitar**. Será necesario el uso de soluciones avanzadas que utilicen diccionarios de términos sensibles (relacionados con orientaciones sexuales, razas, religiones, partidos políticos, enfermedades, etc.) para que los detalles sensibles puedan ser identificados y en su caso, eliminados o protegidos con facilidad.

El remedio

El enmascaramiento de datos o Data Masking surge así como respuesta efectiva a las demandas de confidencialidad y privacidad de la información en los entornos de desarrollo y prueba, formación, soporte, análisis de datos, outsourcing y offshoring, normalmente menos protegidos que los entornos de producción.

¿En qué consiste? Se trata de la transformación de la información sensible en datos que no son verdaderos pero sí verídicos, es decir: mantienen un aspecto similar al real, conservando las propiedades de las datos originales. Estas técnicas permiten alterar los datos de forma aleatoria no determinística, de modo de garantizar la confidencialidad, pero sin perder sus atributos: valor, estructura, formato, relevancia.

Dichos procesos afectan el contenido de nombres, direcciones, campos especiales como el DNI o el número de socio del sistema de salud; teléfono y números de tarjetas de crédito. Para las tarjetas, por ejemplo, genera números válidos y preserva el código identificador del emisor y los dígitos de control. Para los teléfonos, inventa combinaciones aleatorias con el mismo formato. La solución incorpora además reglas y diccionarios especiales para los campos más comunes con información sensible.

Cuando esta opción es un componente de una plataforma de integración completa, la empresa se beneficia además con el acceso universal a los datos, capacidades avanzadas para su transformación y tratamiento y facilidades para la auditoría y el reporting.

Con una herramienta eficaz de enmascaramiento de datos la empresa podrá crear grandes volúmenes de información para mejorar el alcance y la calidad de los entornos de prueba de aplicaciones. El outsourcing y la deslocalización del tratamiento de datos serán opciones más seguras y fiables, y el enmascaramiento abarcará todos los datos sensibles sin importar su origen, reduciendo el riesgo asociado a la seguridad de los datos y al incumplimiento normativo. Además, se podrán reutilizar y estandarizar las reglas de enmascaramiento de datos para múltiples proyectos, obteniendo así un mejor retorno de la inversión.

Box

La Ley 25.326 de Protección de Datos Personales fue sancionada el 4 de octubre de 2000 y en su artículo segundo incluye las siguientes definiciones:

Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

Datos informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

Por su parte, el artículo cuarto establece que “Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención”.

Más información
Dirección Nacional de Protección de Datos Personales
http://www.jus.gov.ar/dnpdpnew/

Datos bajo sospecha

Descubra si su información sensible es confiable y de calidad

Por Josep Tarruella, Director General de PowerData para América Latina
www.powerdataam.com

¿Confía ciegamente en sus datos corporativos? Es muy probable que tenga más de un motivo para sospechar de la calidad de los datos que maneja en su negocio. En los últimos años, la tecnología ha invadido las empresas con múltiples aplicaciones que dependen del uso intensivo de la información, herramientas de business intelligence, CRM´s o sistemas ERP. Sin embargo y con frecuencia, los datos que alimentan a esas aplicaciones son poco fiables, están incompletos y/o imprecisos. Esta problemática –sólo por mencionar un ejemplo- podría conducir a fallos en la cadena de suministro o peor aún: a tomar decisiones de negocio inadecuadas.
Un simple error en los datos de contacto puede hacer perder en un segundo todo lo conseguido gracias a duros esfuerzos en la negociación con los clientes.

Demostrar el impacto de la mala calidad de los datos en el negocio no es una tarea fácil. Cuando se produce una crisis -por ejemplo, en el envío de miles de cartas o emails a clientes inexistentes-, suele cometerse el error de atacar ese problema puntual y dejar de lado la calidad de los datos. Sin embargo, esta "tendencia" puede costar mucho dinero a las organizaciones.

Si quiere saber hasta qué punto puede confiar en sus datos, responda este sencillo test que le ayudará a identificar un posible foco de peligro.

¿Tiene problemas para establecer la procedencia de algún dato? ¿No sabe cuánto tardará en encontrar un dato, tiene dudas sobre su exactitud o qué modificaciones ha sufrido?
Este problema se presenta con frecuencia cuando se intenta implementar cualquier sistema de gestión –tal vez para el área de Recursos Humanos o finanzas, o frente a una auditoría. Los datos pierden integridad y sus vínculos de asociación. En este escenario es de vital importancia migrar sólo los datos precisos, adecuados y actualizados, conocer su procedencia e idealmente qué cambios se les han hecho.

¿Cuándo solicita el balance de ventas de un período determinado a tres áreas, cada informe muestra resultados distintos?
Nadie sabe a ciencia cierta qué datos están almacenados en un formato no estándar; cada área parece hablar un lenguaje de negocio diferente por lo que tomar una decisión resulta complejo y arriesgado. Cada área tiene una visión distinta de un cliente: el área de finanzas lo ve como un numero neto: el area de facturación, como un pagador: el departamento comercial, como un todo (no ve si el cliente es rentable o no, ni los descuentos): consultoría ve sólo los servicios. La realidad es que un cliente debe ser el mismo para todos, todos deberían tener la misma información para conocerlo bien y así tomar las decisiones adecuadas en relación a este.

¿Ha sufrido alguna vez las consecuencias de un error de inventario? ¿Un camión dejo productos en un lugar equivocado o fuera de hora?
El inventario se confeccionó conforme a un listado provisto por el departamento logístico. Sin embargo, Ventas maneja otros datos y, finalmente, se entregan productos a un cliente que no los había facilitado. En algún momento de la cadena la información se deterioró, se volvió inconsistente y por ende, perdió su valor.

¿Aceptó nuevamente a un cliente que no es buen pagador?
El departamento de riesgos olvidó actualizar la lista de morosos. El costo del error no tardará en reflejarse en la tabla de resultados.

¿El 15% de un envío masivo para la campaña de marketing resultó devuelto?

Es uno de los casos más frecuentes en los que se refleja la mala calidad de los datos Los contactos pueden estar duplicados, haber cambiado de domicilio e, incluso, haber fallecido sin que se hayan recogido esos cambios en la base de datos.

Los datos deteriorados no mejoran por si solos, sino que degeneran rápidamente a lo largo del tiempo, distorsionan la realidad y dificultan la toma de decisiones. En todos los escenarios descritos, los metadatos (esenciales para comprender la estructura de los datos) nos indicarán qué información falta o cuál es útil para nuestros propósitos. Por otro lado, el uso extensivo del perfilado permitirá examinar valores individuales y encontrar su forma, frecuencia, tipología y distribución. Servirá además para identificar los valores correctos, el tiempo (buscando patrones en datos históricos y su evolución en diferentes períodos), la transición de estados y la dependencia (reconocimiento por patrones para identificar relaciones ocultas entre atributos). También serán muy útiles las validaciones recurrentes de los datos y la comparación con fuentes fidedignas.
Se trata, en definitiva, de ver la calidad de los datos como una inversión vital para el negocio; de velar por su integridad a lo largo de todo el ciclo de vida, de estar informado sobre el grado de deterioro para identificar las áreas críticas antes de que se produzca una crisis y el costo para el negocio sea inevitable.

aleph comunicación

CONTACTO DE PRENSA

Muriel Mirvois
4556-1467 / 15 6106-6560
muriel@alephcom.com.ar

María Laura Pacheco
15 6504-9677
laura@alephcom.com.ar