ISNN 999-4605

Organización de los Estados Americanos
Organização dos Estados Americanos
Organisation des États Américains
Organization of American States

79
EDICION

FORO e-GOBIERNO OEA | BOLETÍN

NOVIEMBRE 2012

e-Gobierno y Gestion de Identidades

IDRC CRDI

Canadian International Development Agency
Agence canadienne de développement international

Canada

TABLA DE CONTENIDO

CRÉDITOS

Miguel A. Porrúa
Coordinador e-Gobierno, OEA

José Luis Tesoro
Responsable Foro e-Gobierno, OEA

Javier Sáenz Coré
Indagación de enlaces Web, OEA

Daniela Paoli
Oficial e-Gobierno, OEA

EDITORIAL

Una de las cuestiones que condicionan críticamente la evolución del e-Gobierno reside en la acreditación de identidad para efectuar trámites que requieren elevados niveles de confiabilidad acerca de que el usuario es efectivamente quien afirma ser y que está habilitado para tramitar lo que requiere.

Se entiende por identidad al conjunto de rasgos propios que caracterizan a una persona en relación a las demás. Dentro de una sociedad, la noción de identidad es inherente a la persona, dado que sólo se considera como tal y sujeto de derecho a quien posee una identidad registrada por el Estado, con nombre y apellido, sexo, filiación, nacionalidad, fecha de nacimiento, fisonomía, características personales, domicilio, estado civil, entre otras. La identificación indubitable de las personas es una función esencial e indelegable de los Estados nacionales.

La creciente utilización de las TIC, en las diversas faces de nuestras vidas, impone la prioridad de garantizar la identidad digital, así como de prevenir y evitar los riesgos que puedan afectarla en sus distintas manifestaciones. Entre los riesgos más notorios se destacan la adulteración o usurpación con fines ilícitos, así como las amenazas a la privacidad y los datos personales.

La notoria evolución de las tecnologías biométricas permite alcanzar crecientes niveles de confiabilidad, mediante el reconocimiento de huellas dactilares, patrones faciales o palmares, de voz, retina, iris o ADN, así como de combinaciones multi-biométricas. El equipo de e-Gobierno de la OEA y la Red GEALC promueven y facilitan el intercambio de experiencias y las herramientas TIC necesarias para apoyar estos procesos. Entre estos aportes de la OEA, merece especial atención el Programa de Universalización de la Identidad Civil en las Américas (PUICA), que ha contribuido a dotar de identidad a millones de personas de la región.

En este número del Boletín, referido a la gestión de identidades en servicios de e-Gobierno, presentamos relevantes testimonios, así como documentos y notas pertinentes. Confiamos en que su diseminación contribuya a promover el aprovechamiento del potencial de las herramientas pertinentes en los países de América Latina y el Caribe, en beneficio del desarrollo del e-Gobierno y de nuestras sociedades.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA)

Secretaría de Asuntos Políticos (SAP)

Departamento para la Gestión Pública Efectiva

TEMA DEL MES: **e-Gobierno y Gestión de Identidades**

ENTREVISTAS

Entrevista a Steven Griner, Coordinador del Programa de Universalización de la Identidad Civil en las Américas (PUICA), Departamento para la Gestión Pública Efectiva, Secretaría de Asuntos Políticos, OEA

Por José Luis Tesoro

1.- ¿Cómo percibe usted comparativamente la prioridad asignada a la gestión de la identidad civil en América Latina y en otras regiones del mundo?

En los últimos seis años la tasa de subregistro en las Américas ha disminuido del 18% al 10%, ubicando a la región en mejor posición que otras del mundo. Según datos de UNICEF, la tasa de subregistro en África subsahariana alcanza el 62%, en Asia llega al 55% y en el Medio Oriente y África del Norte se encuentra en 23%. Esas estadísticas, sin embargo, no cuentan toda la historia. Cabe recordar que anualmente 1.3 millones de nacimientos en las Américas no son registrados y que aproximadamente 6.5 millones de niños no cuentan aún con certificado de nacimiento. Se estima además que un número similar de adultos no posee documentación adecuada para el ejercicio de sus derechos fundamentales. El subregistro predomina entre los hijos de madres solteras, muchas de las cuales tampoco poseen documentos de identidad. Un niño que no cuenta con un certificado de nacimiento es menos proclive a recibir servicios de educación y salud y más propenso a ser abandonado o explotado.

2.- ¿Podría proporcionarnos una reseña de los objetivos, estrategias y resultados del Programa para la Universalización de la Identidad Civil en las Américas (PUICA)?

El 2008 la Asamblea General de la OEA aprobó el Programa Interamericano para el Registro Civil Universal y Derecho a la Identidad para el fortalecimiento de los sistemas de registro civil y la universalización del registro civil. Hoy en día el PUICA implementa proyectos en 17 Estados Miembros de América Central y del Sur y del Caribe. Dos prioridades, identificadas por los mismos países, son la implementación del registro hospitalario permanente y las campañas en zonas fronterizas.

Si bien no existe una receta única para eliminar el subregistro, la implementación de oficinas registrales en los servicios de maternidad de los hospitales contribuye a disminuir el subregistro en el preciso momento del nacimiento y sirve como un punto de encuentro, tanto para los futuros padres y madres como para el personal hospitalario y otros promotores comunitarios. No es casualidad que en aquellos países con una extensa red de oficinas hospitalarias la indocumentación infantil sea prácticamente nula, como son los casos de Uruguay, Argentina y Costa Rica, entre otros.

Con el propósito de reducir aun más la tasa de subregistro, PUICA ha enfocado sus esfuerzos en campañas en las zonas fronterizas, cuyas poblaciones son desproporcionadamente más proclives a no contar con documentos de identificación. En estas actividades, las unidades móviles emiten documentos o corrigen errores en la información de los registros en comunidades fronterizas en Ecuador, Perú, Paraguay y Bolivia.

3.- ¿Qué potencial percibe en las herramientas de e-Gobierno y de las TIC en materia de gestión de identidad civil?

Hasta recientemente, la mayoría de los procedimientos de los registros civiles se realizaban de manera manual. La información se incluía en grandes libros de registro, a menudo archivados en las municipalidades que tenían bajo su responsabilidad la inscripción de nacimientos, defunciones y matrimonios. La mayor parte de los países de las Américas han iniciado procesos de automatización de registros en bases de datos centralizadas, usando versiones escaneadas de los registros originales para verificar la veracidad y exactitud de la información. Eventualmente, los registros civiles expandirán la interconexión de sus oficinas para facilitar el registro en las regiones más alejadas y suministrar a otras entidades gubernamentales información actualizada sobre estadísticas vitales.

4.- ¿Cuál es el escenario previsible en el mediano plazo en materia de aplicación de herramientas de e-Gobierno y de TIC en la gestión de la identidad civil?

En esta época informática, no es suficiente con poseer un certificado o tarjeta de identificación, dado que los ciudadanos realizan una miríada de transacciones comerciales, sociales y políticas, posibilitadas solo por una identidad localizable y verificable. Estas transacciones y la información generada están creciendo exponencialmente; de hecho, 90% por ciento de toda la data del mundo ha sido producida durante los últimos dos años. A medida que los desafíos de interoperabilidad informática y de protección de datos se tornen más complejos, la automatización de la identidad civil continuará a un paso aún más acelerado.

Entrevista a Ramón Gerónimo Brenna, Profesor de Posgrado en el Programa de Actualización en Derecho Informático -en línea- de la Facultad de Derecho de la Universidad de Buenos Aires

Por José Luis Tesoro

1.- ¿Cómo percibe usted la prioridad asignada a las cuestiones atinentes a la gestión de identidades en América Latina?
Dado que la creciente presencia de personas y entidades en Internet ha generado un escenario de gran interacción y distribución global[1], la gestión de identidades es un factor fundamental para el desarrollo de las economías digitales o en red.

La identidad de los individuos esta compuesta por elementos destinados a garantizar la unicidad de una persona física y por elementos que son la expresión de la identidad humana, en todos sus posibles aspectos.
Legalmente, la **identidad personal** está conformada por el conjunto de datos resultantes de la unión de información relativa a una persona, que se encuentra en los registros públicos, información que se pretende permita identificarla de manera unívoca.

El concepto de identidad digital o identidad en la Red, tiene su origen en la interacción de los usuarios con los servicios que les son ofrecidos a través de la Red. Contiene, por un lado, los datos de acceso, como el nombre del usuario y su contraseña, y por otro parámetros tales como la información a la que quieren acceder, sus necesidades y preferencias, pues estos datos son personalizados por los prestadores y utilizados por ellos, como medio adicional de identificación de los usuarios de sus servicios, pues reflejan aquella identidad.

En ese entorno, marcadamente digital y global, no nos debe sorprender que la gestión fiable de identidades represente un punto central para alcanzar un traslado garantizado de los procesos y transacciones tradicionales del mundo del "papel" (con medios de identidad tradicionales) al ámbito digital de la Red.
Muchas personas aspiran hoy a disponer de una identidad única e integrada en la Red, representada por una credencial también única, que les permita acceder a todos los servicios ofertados en aquélla,

[1] Un 32,5 % de la población mundial ya tiene acceso a Internet según un informe presentado por la ONU, que sitúa a Islandia, Noruega, los Países Bajos, Suecia, Luxemburgo y Dinamarca como los únicos países con más del 90 % de sus habitantes conectados a la red. Unión Internacional de Telecomunicaciones (UIT), sexta reunión de la Comisión, celebrada en Nueva York en Septiembre de 2012.

con prescindencia de que sean ofrecidos por un proveedor público, gubernamental, o uno privado, o que el servicio pueda ser catalogado de público o privado.

Para responder a tales expectativas, los países deberán dotar a sus ciudadanos de una identidad "digital" que les permita identificarse en la Red con las mismas garantías y seguridad con que lo hacen en las relaciones interpersonales tradicionales.

En este aspecto cabe reconocer la existencia de una distancia muy importante en los avances, entre los países con mayor desarrollo –EE.UU. y Unión Europea- y los de nuestra área.

2.- ¿Cómo califica usted el estado actual de las técnicas de gestión de identidades en América Latina? ¿Cuáles son los factores internos y externos que impulsan y condicionan los avances en la materia?

Si nos enfocamos en América Latina, lo primero que notamos es una gran asimetría. Algunos países carecen, aún hoy, de una gestión confiable de identidades con medios tradicionales.

Esto marca una dificultad inicial, que se presenta como un factor interno que obstaculiza un desarrollo armónico y eficiente de las nuevas técnicas. Un panorama similar se presenta en el acceso a las TIC, con marcadas asimetrías entre nuestros países.

Esas dificultades se suman y se portan del mismo modo a los posibles emprendimientos, dado que lo que se observa también, en muchos casos, es la ausencia de políticas de Estado dirigidas a resolver estos problemas.

Faltan asimismo, y probablemente por las mismas razones, planes comunes a los países del área, o en los mercados ampliados como el Mercosur y otros de la región. Si esta situación no se revierte dentro un plazo razonable, afectará al desarrollo de nuestras nuevas economías digitales e incrementará costos a nuestros ciudadanos.

Pero al mismo tiempo, los notorios avances en la globalización y en la economía de red generan nuevos retos que deben ser resueltos en términos de identidad y su gestión.

De hecho, en la Red se ha desarrollado un sistema, que podríamos llamar "privado", constituido por proveedores que -al interactuar con ellos- nos autentican y gestionan los datos que les entregamos de manera voluntaria. Accedemos a sitios, proveemos datos de identidad personal y otros adicionales y, con base a ellos, se nos proporciona una clave para acceder y usar las respectivas prestaciones, dentro de un sistema relativamente inseguro, que prácticamente carece de supervisión, y que puede o no proteger adecuadamente nuestra identidad y nuestra privacidad. Los ciudadanos de nuestros países exhiben creciente adhesión a este sistema sin el respaldo y cuidado de sus Estados.

También existe otro sistema privado, pero con un grado de supervisión mayor. Es el caso de la NSTIC (National Strategy for Trusted Identities in Cyberspace), proyecto del gobierno de los EEUU que procura combinar las iniciativas privadas de las que hablábamos, con las que derivan de la protección de los consumidores.

Por último, hay un enfoque más público del problema, cuando los gobiernos de un grupo de países deciden trabajar juntos para proporcionar las soluciones que la identidad les presenta a la nueva economía. Es este el sentido que se le ha dado al tema, en la Unión Europea. Se trataría aquí de la creación de un sistema de identidad gubernamental que nos permita acceder a los servicios proporcionados por las Administraciones y que a su vez pueda ser utilizado por los privados. Un ejemplo de esto último lo encontramos en el "eGovernment Action Plan 2011-2015", de la Comisión Europea**.**

Recordemos que el Estado tiene dos roles fundamentales en este proceso: como custodio de la información de los ciudadanos y como proveedor de información y servicios esenciales. Desearíamos que los gobiernos de nuestros países reconocieran la necesidad de ejercer efectivamente esos roles y la incluyeran en la agenda regional como una prioridad. Esto requerirá un esfuerzo importante de armonización y homogeneización de los sistemas de identidad de los distintos países, a partir de estándares comunes que aseguren confiabilidad y seguridad.

3.- ¿Cuáles es el potencial previsible de las herramientas de e-Gobierno y de las TIC en materia de gestión de identidades y biometría?

El potencial es inmenso, dado que el e-Gobierno se basa en una gestión adecuada de identidades y las TIC aportan elementos esenciales para ello.

En lo privado hay un gran desarrollo en la última década en materia de seguridad en los accesos y en las transacciones entre usuarios y empresas; hoy con fuerte presencia de aplicaciones biométricas.

En lo público, se verifica el desarrollo de iniciativas para introducir identidades electrónicas –eID- en los servicios públicos con los correspondientes sistemas de gestión de esas identidades, habiéndose enfatizado -más recientemente- en la compatibilidad entre esos sistemas,

Se está difundiendo la implantación de tarjetas de identificación electrónicas -ID cards- que contienen un chip que almacena información digital acerca de la identidad de su titular, así como la interacción con ciertas aplicaciones, de manera que el titular pueda acreditar identidad y que la misma pueda ser verificada y controlada digitalmente. En sus versiones más avanzadas incorporan datos biométricos del titular, tales como su huella digital, particularidades de su rostro u otros parámetros anatómicos o fisiológicos.

Estos nuevos elementos de identificación permiten superar el estancamiento que presentaban en su evolución los medios tradicionales de identificación de personas, como los documentos nacionales de identidad, las tarjetas de ciudadano, etc. Aún los más avanzados, producidos con nuevas medidas de seguridad anti falsificación, presentan la limitación de ser válidos sólo ante instituciones oficiales y empresas del país emisor, pero poco útiles en la Red.

Es por ello que insistimos en la prioridad de encarar proyectos comunes que permitan evolucionar hacia una identidad electrónica o digital reconocida más allá de las fronteras nacionales, en un mercado común, en una comunidad de países, o por qué no, con alcance global.

Se trata de una cuestión estratégica para que nuestros países puedan ingresar y desarrollar sus economías en estos nuevos espacios. Las eID cards pueden proporcionar esta solución, pero su concreción requiere políticas comunes y acuerdos.

Cabe reiterar que, hasta hoy, padecemos barreras u obstáculos que no permiten un desarrollo más apropiado de este tema: las asimetrías, la falta de políticas de Estado, la ausencia de planes y proyectos comunes entre nuestros países, el temor al robo de identidad y al fraude, así como las dudas sobre las garantías de privacidad y uso correcto de los datos personales de identidad.

Sin embargo, dada la relevancia presente y futura de una gestión eficiente de identidades digitales, nuestros Gobiernos deben darse políticas armónicas y homogéneas, así como trabajar juntos para encontrar las soluciones más adecuadas.

La difusión de los dispositivos móviles y la gestión de identidad en la nube tornan aún más aguda esta cuestión para la seguridad de redes y la continuidad y expansión del negocio en red. El hecho de que cada vez más empleados lleven a su trabajo sus dispositivos móviles *("Bring-your-own-device, BYOD")*, está generando un nuevo problema que se expande rápidamente, y que afecta prácticamente a todas las organizaciones.

Del mismo modo, la nube es acompañada por una pérdida de control de la gestión del acceso de usuarios y sus identidades. Tanto las ofertas de "autenticación simple" *("single-sign on"*) como las de "software como servicio" (SaaS) representan un desafío para la mayoría de las organizaciones, en especial para las principales de EE.UU., donde todas las áreas de empresas requieren, de manera creciente, acceso a las nuevas aplicaciones alojadas en la nube.

No resulta extraño entonces que se identifiquen, en este año 2012, cuatro grandes preocupaciones en las que centrarse: (i) la seguridad de los dispositivos móviles, (ii) la gestión de identidad dentro de la nube, (iii) la gestión de perfiles y amenazas, y (iv) las crecientes presiones regulatorias gubernamentales. Se trata de cuatro cuestiones estratégicas en las que debe avanzarse. La gestión de identidad y la privacidad se presentan como más importantes que nunca antes, pero también como más problemáticas. Las aplicaciones biométricas adicionan problemas nuevos a resolver. Hay cierto desconocimiento y muchos prejuicios por vencer.

Entonces la pregunta a responder es ¿cómo evolucionar? Siguiendo la experiencia de estos años y teniendo en cuenta las deficiencias que se han manifestado recientemente, podemos delinear algunas líneas de acción:

a.- Una de las principales causas del fracaso de los proyectos de gestión de la identidad ha sido contar con un ámbito de aplicación demasiado amplio combinado con una falta de enfoque en el valor del negocio en la Red. Por ello, las iniciativas deben ser limitadas en su alcance y deben tener en cuenta las propiedades del cronograma preciso a seguir y el presupuesto asignado. Es aconsejable concretar pasos más pequeños pero seguros hacia nuestro objetivo, dado que nos impulsarán a seguir.

b.- Aumentarán las demandas de una autenticación más fuerte y de infraestructuras de identidad más sólidas y coordinadas. Hemos verificado empíricamente la existencia de serias deficiencias en ambos aspectos. Los ciudadanos usuarios y las organizaciones públicas y privadas, necesitan saber en qué están confiando, por qué y para qué. También necesitan saber cuáles serán las consecuencias si las organizaciones a las que se confía información sobre identidad no cumplen con sus obligaciones, o no respetan nuestra privacidad y dan un uso incorrecto o directamente ilegal a nuestros datos.

c.- Los requisitos de autorización se han vuelto más complejos y más urgentes, para dar respuesta a las crecientes presiones reguladoras. Los entornos de TIC y de la economía en Red incorporan mayor riesgo y mayor complejidad. La utilidad de las identidades se basa en la autorización del acceso y en la creación de registros. Si esto es así, esta área asumirá una posición central y preponderante, con alto potencial de desarrollo en el futuro inmediato.

d.- Las aplicaciones biométricas se expandirán y ofrecerán una interesante oportunidad de trabajo y negocio. Los avances tecnológicos para identificación biométrica han sido notables durante los últimos cinco años; las unidades de reconocimiento facial, de pupilas y de huellas dactilares ya están incorporadas en una gran cantidad de dispositivos que usamos a diario y con los cuales interactuamos en muchos lugares: edificios, discotecas, esquinas de las grandes ciudades, supermercados del primer mundo y dispositivos de identificación ciudadana en procesos electorales (voto electrónico, voto por Internet). Hay también un buen número de aplicaciones pensadas como soluciones de seguridad en el mercado del comercio electrónico, del comercio en la Red, para la validación de firmas digitales, el marketing personalizado y la seguridad de las ciudades. Juegan un papel muy importante en el control en zonas fronterizas, puntos de inmigración y aeropuertos. La tecnología biométrica ofrece en estos espacios un mecanismo eficiente de identificación, con la capacidad de cotejar datos con cientos de bases de datos disponibles a escala global.

e.- Es necesaria la integración. La gestión de identidad debe comenzar a cerrar la brecha entre las organizaciones y los ciudadanos. La gestión de identidades federadas, como hemos visto, es una tarea compleja, y aún son inmaduros los protocolos y atributos para la provisión y gestión federada de las políticas de identidad. Pero la brecha existente en la arquitectura de la identidad moderna está comenzando a cubrirse y debe constituirse en un puente por el que transite la información referente a identidades.

f.- Las amenazas derivadas de la afectación a la privacidad y el robo de identidad son temibles para el gran público y provocan alarma y cierta inacción, invistiendo un grave impacto en las operaciones comerciales e incluso en la viabilidad del negocio en Red y la nueva economía. La comunidad empresarial y los gobiernos que pugnan por el cumplimiento de la ley seguirán en clara disputa en el futuro próximo, pero esperemos que esa disputa impulse los cambios deseados en la infraestructura de identidad.

4.- ¿Cuáles son las características de las iniciativas más promisorias en materia de aplicación de herramientas de e-Gobierno y de TIC en gestión de identidades y biometría en América Latina y en el mundo?

Como una de las primeras iniciativas puedo mencionar el Modinis eIDM Study, cuyo principal aporte para la interoperabilidad de los sistemas de gestión de identidades ha sido la definición de una infraestructura de alto nivel, un modelo o marco conceptual, denominado Modinis Conceptual Framework, es decir un portal basado en federación, que recoge las principales propuestas realizadas en el proyecto, en cuanto a organización general y principios básicos que deben regir una infraestructura eIDM a nivel Europeo. La infraestructura se basa en un modelo federado que confía, en una serie de portales de identidad de cada Estado, la responsabilidad de autenticar a una entidad y de decidir acerca del nivel de confianza que se asigna a los procedimientos de autenticación.

Otro sistema es el denominado TLS- Federation, cuya función central es la autenticación, desarrollando en menor medida la identificación y la autorización. Para la autenticación se usa una implementación estándar de TLS y se puede utilizar una I-Card, que es una pieza de software que corresponde a una identidad digital de un usuario, almacenada en un archivo. No está limitada en longitud, tamaño y capacidad. Gira además en torno a certificados basados en PKI y al uso de tarjetas inteligentes que requieren estándares adicionales como el PKC#11 y CSP (crytographic service provider).

Muy importante también ha sido el proyecto GUIDE (Creating a European Identity Management Architecture for eGovernment) que se propuso desarrollar un modelo para la interoperabilidad en materia de identidad que permitiese, a los Estados miembros de la UE, confiar en la identidad de una entidad (ciudadanos- empresas) de otro Estado. Se trataba de alcanzar una Red federada de identidad, cuidando privacidad y dando seguridad a los intercambios de información; un canal de confianza.

Otra propuesta para mencionar es STORK (Secure idenTity acrOss boRders linKed) que trata de desarrollar y probar especificaciones comunes para el reconocimiento seguro de las identidades electrónicas- eID- nacionales de los países involucrados. Se basa en un modelo federado de interoperabilidad tecnológicamente neutral y con múltiples niveles de autenticación.

En la actualidad, los sistemas de gestión de identidad se dirigen a la federación y el multinivel, para que puedan convivir tarjetas de identificación con usuarios y contraseñas.

Ahora bien, la asimetría también está presente todavía en Europa, donde pueden apreciarse claras diferencias entre experiencias nacionales; unas más avanzadas y otras incipientes. Por ello son fundamentales la federación, la utilización de estándares comunes, el multinivel y el respeto a la privacidad.

Existen problemas comunes a resolver; entre ellos: (a) la duplicidad de fuentes de datos, que genera incoherencias y duplicidad de información; (b) el acento en las aplicaciones de e-Gobierno deja afuera al sector privado, lo que resulta conflictivo con la posibilidad de que la participación del sector privado -entidades bancarias, empresas de servicios o de consumo, etc.- juegue un papel dinamizador en el desarrollo de estos sistemas de identidad digital; y (c) la insuficiente atención a las cuestiones vinculadas a la delegación de identidad, la delegación de autorización y el manejo de diferentes roles; dado que muchas transacciones son ejecutadas por representantes legales que actúan en nuestro nombre ante administraciones y sector privado, y uno mismo puede tener distintos roles simultáneos dentro de un sistema de gestión de identidades.

Para finalizar, en este año, según versiones periodísticas[1], la Unión Europea se ha propuesto revisar sus normativas sobre identidad y firma electrónica. Entre las propuestas de Bruselas se encontraba la de obligar a los países a reconocer entre sí las tarjetas de identidad electrónica de los ciudadanos. Además, se proponía la creación de organismos de supervisión para evaluar la tecnología de verificación. De acuerdo con algunas informaciones, las propuestas de Bruselas se dirigían a crear un sistema ID electrónico obligatorio para todos los ciudadanos de la UE, pero las autoridades de la Comisión no han confirmado tal extremo, probablemente debido a que sus responsables son conscientes de que las propuestas pueden levantar la oposición del Parlamento Europeo y de algunos grupos de derechos civiles, debido al temor a que se puedan producir robos de identidad y fraudes virtuales.

Si bien estos delitos han crecido de manera preocupante y justifican de algún modo aquel temor, creemos que los sistemas de gestión de identidad pueden aportar soluciones también a estos nuevos problemas de la Red. Dado que las decisiones de los actuales responsables determinarán nuestro futuro de crecimiento y desarrollo, debemos acertar.

[1] Network World, Fecha: 05/06/2012

Entrevista a César López, Especialista en gestión de identidad y biometría; ex CIO del Registro Nacional de Identidad y Estado Civil (RENIEC), Perú

Por Juan Carlos Pasco

1.- ¿Cómo percibe usted comparativamente la prioridad asignada a la gestión de identidades en América Latina y en otras regiones del mundo?

La prioridad asignada a la gestión de la identidad de las personas está estrechamente vinculada con la idiosincrasia de las comunidades. La sucesiva maduración de tal prioridad se asocia a la implementación de mecanismos de registro de ciudadanos para el ejercicio de derechos sociales y cívicos, tales como el sufragio electoral. En países como Japón, donde predomina una atmósfera de confianza, las personas se identifican cotidianamente con sus tarjetas de crédito o carnés de servicios, manifestando una notoria renuencia al uso de un documento de identidad que pueda asociarlas a un número de registro. Otro caso interesante es el de países europeos como Alemania y Francia, cuyos marcos regulatorios y leyes de privacidad personal –provenientes de la postguerra- impiden el uso de técnicas biométricas para autenticar la identidad, si bien son –paradójicamente- los principales proveedores de ese tipo de soluciones biométricas.

En países de Latinoamérica, Asia y África, con un alto legado de tasas de sub registro (ausencia de registros de nacimiento), se viene asignando alta prioridad al fortalecimiento de los registros civiles y de identidad. Como primer paso se adoptaron procesos de registro automatizados que pueden incorporar técnicas biométricas con fines de validación de identidad.

Queda claro entonces que la prioridad asignada a los sistemas de registro de identidad está condicionada por la idiosincrasia y los legados históricos de cada nación. En el caso del Perú, los registros electorales municipales se incorporaron en 1995 a través del Registro Nacional de Identidad y Estado Civil (RENIEC), organismo constitucionalmente autónomo que forma parte del Sistema Electoral, con personería jurídica de derecho público interno y atribuciones en materia registral, técnica, administrativa y financiera, cuya finalidad principal es fortalecer la seguridad jurídica organizando y manteniendo el Registro Único de Identificación de las Personas Naturales (RUIPN) e inscribiendo los hechos y actos relativos a su capacidad y estado civil. El RENIEC fue designado en 2008 como la entidad de certificación raíz y primera emisora de certificados digitales del Estado Peruano como base para la implementación de la identidad digital para uso de servicios de e-Gobierno.

2.- ¿Cuáles son los factores internos y externos que impulsan y condicionan los avances en la gestión de identidades en Perú y en América Latina?

Con relación a factores internos, cada país –de acuerdo con su propia problemática- opta por alternativas de mejora en procesos e infraestructura tecnológica que favorezcan a los ciudadanos en el ejercicio de sus derechos fundamentales así como a la seguridad jurídica del país. En este marco, las instituciones a cargo de la implementación de políticas de Estado, han propiciado el desarrollo de sistemas de información de registros civiles y de identidad orientados a tener plenamente identificada a la totalidad de la población.

En el Perú, durante los años 2004 a 2010, se diseñaron, desarrollaron e implementaron los sistemas de información de registro de identidad y de registro de hechos vitales (SIO y Sistema de Información de Registro Civiles). Asimismo, desde 2005 se ejecutó uno de los proyectos mas importantes de Estado denominado Proyecto de Restitución de Identidad, mediante el cual se logró pasar de un 65% de población identificada con DNI al 99.2 % en poco mas 4 años. En 2006 se inicio la implementación del sistema de identificación basado en impresiones dactilares (AFIS), identificándose a más de 18.000 personas que tenían más de un registro de identidad, llegando así a contar con un Registro Único de Identidad de Personas Naturales (RUIPN) de alta confiabilidad.

Respecto de factores externos, debería contarse -en un futuro cercano- con capacidades de interoperabilidad entre los distintos sistemas de identificación en el ámbito regional, contemplando el uso de búsquedas mediante componentes biométricos (1:1 y 1:N), lo cual estará asociado al nivel de madurez de la gestión de identidad en cada país y en la adopción de buenas prácticas sujetas a estándares técnicos internacionales

Resulta ya evidente el favorable impacto de las técnicas de gestión de identidades, al facilitar notoriamente el acceso de los ciudadanos al ejercicio de sus derechos y a los servicios prestados por instituciones estatales y del sector privado.

3.- ¿Cuál es el potencial de la gestión de identidades para favorecer el uso de prestaciones de e-Gobierno? ¿Cuáles son los servicios ofrecidos por el RENIEC del Perú con base en dicho potencial?

El potencial de las herramientas de e-Gobierno esta críticamente limitado por la posibilidad de identificar a los ciudadanos participantes en transacciones digitales como las canalizadas vía Internet.

Una opción reside en implementar infraestructuras basadas en claves públicas (*Public Key Infrastructure, PKI*) que permitan el uso de certificados digitales equivalentes -en el mundo digital- a los documentos de identidad de las personas, los cuales identifican plenamente a los participantes y permiten el uso de firmas digitales que tienen el mismo valor legal que las firmas manuscritas en papel. Esta opción exhibe experiencias exitosas en países como Finlandia, España y Estonia, entre otros. En el ámbito latinoamericano tenemos a Brasil como caso de éxito y en el Perú contamos, a la fecha, con todo el marco normativo y tecnológico para garantizar una implementación exitosa del uso de certificados digitales, considerando que el proyecto de DNI Electrónico está próximo a ser lanzado.

El RENIEC ha implementado los siguientes servicios biométricos:

- Sistema de identificación biométrica para transacciones de compra y venta notarial (2008): servicio a disposición de los notarios públicos para validar la identidad de los participantes de una transacción comercial de compraventa de vehículos o inmuebles, mediante una verificación biométrica basada en la impresiones dactilares (1:1) comparando la huella capturada digitalmente de cada persona (asociada a al número de documento de identidad) con la almacenada en las bases de datos del RENIEC.

- Kioscos Multimedia para emisión de partidas registrales de nacimiento y registros civiles; plataforma de pagos de servicios, y de solicitud de duplicados de DNI (2008): dichos servicios tienen como fase inicial de los trámites la identificación biométrica del solicitante (1:1).

- RENIEC Identifica (2009): servicio prestado a la comunidad a través de unidades móviles para verificar la identidad de personas anónimas (NN) en situaciones de emergencia, accidentadas o fallecidas, con el propósito de contactar a sus familiares cercanos. Esta búsqueda biométrica es del tipo "uno a muchos" (1:N), tomándose las huellas del individuo afectado y comparándolas con todas las huellas de la base de datos de identidad.

- Verificación de identidad de delincuentes o personas procesadas (2010): servicio del tipo "uno a muchos" (1:N) puesto a disposición de la Policía Nacional, del Ministerio Público, del Instituto Nacional Penitenciario y del Poder Judicial del Perú.

4.- ¿Cuáles son las características de las iniciativas más promisorias en materia de aplicación de e-Gobierno y de TIC en gestión de identidades y técnicas biométricas?

Las capacidades disponibles en materia de e-Gobierno y TIC permiten mejorar la descentralización de registros de identidad, por ejemplo a través de estaciones móviles que transitan comunidades rurales, con posibilidad de verificar en línea la eventual existencia de registros anteriores asociados a una misma impresión dactilar. Asimismo, resulta sumamente efectivo el uso de sistemas de información geo-referencial (GIS) para determinar los accesos y vías de comunicación para desplegar programas de registro de identidad en todo el territorio nacional, así como para detectar "bolsones" de población por identificar. Las aplicaciones GIS, al asociar vistas geo-referenciadas de diversas capas, permiten concretar valiosas sinergias con otros programas asociados a diversas políticas de Estado, tales como alfabetización, lucha contra la pobreza, atención materno-infantil, mejora del hábitat, entre otros.

Respecto de las técnicas biométricas, cabe señalar que si bien las tradicionales (TIR) llegan a identificar a personas con un nivel de efectividad del orden del 95%, muchos países están optando por la verificación biométrica cruzada, utilizando al menos dos características biométricas complementarias. Por ejemplo, el proyecto de identificación de India (IUDAI) utiliza las impresiones dactilares y el iris ocular para la identificación de su población. Cabe agregar que hoy existen nuevas técnicas de reconocimiento de impresiones dactilares -tales como MSI (Multi-Spectral Images-.que alcanzan un nivel de precisión del 99.6%, al incorporar la primera capa vascular del dedo como rasgo adicional de reconocimiento.

A la fecha muchos países en Latinoamérica, Asia y África han optado por formatos de documento de identidad electrónicos (eDNI), de contacto (smartcards), sin contacto (radio frecuencia - RFID) o hibridas (combinadas), algunos de ellos con capacidad de almacenar certificados digitales con firma electrónica.

Los documentos de identidad electrónicos tienen, en muchos casos, una función de validación biométrica denominada MOC (Match on Card), que permite comparar la huella digital con la almacenada en los registros nacionales. Entre los países que han implantado este tipo de soluciones tenemos a España, Guatemala, India, Nigeria, Chile, Brasil entre otros.

Respecto de las técnicas biométricas, cabe señalar que si bien las tradicionales (TIR) llegan a identificar a personas con un nivel de efectividad del orden del 95%, muchos países están optando por la verificación biométrica cruzada, utilizando al menos dos características biométricas complementarias. Por ejemplo, el proyecto de identificación de India (IUDAI) utiliza las impresiones dactilares y el iris ocular para la identificación de su población. Cabe agregar que hoy existen nuevas técnicas de reconocimiento de impresiones dactilares -tales como MSI (Multi-Spectral Images-.que alcanzan un nivel de precisión del 99.6%, al incorporar la primera capa vascular del dedo como rasgo adicional de reconocimiento.

A la fecha muchos países en Latinoamérica, Asia y África han optado por formatos de documento de identidad electrónicos (eDNI), de contacto (smartcards), sin contacto (radio frecuencia - RFID) o hibridas (combinadas), algunos de ellos con capacidad de almacenar certificados digitales con firma electrónica.

Los documentos de identidad electrónicos tienen, en muchos casos, una función de validación biométrica denominada MOC (Match on Card), que permite comparar la huella digital con la almacenada en los registros nacionales. Entre los países que han implantado este tipo de soluciones tenemos a España, Guatemala, India, Nigeria, Chile, Brasil entre otros.

Entrevista a Santiago Paz, Director y fundador del Centro Nacional de Respuesta a Incidentes de Seguridad Informática de Uruguay (CERTuy)

Por Cristina Zerpa

1.- ¿Cómo percibe usted la importancia de la identidad digital para el desarrollo del gobierno y del comercio electrónico?

El gobierno y el comercio electrónico permiten a los usuarios efectuar transacciones de manera remota –a través de las TIC- sin necesidad de trasladarse. Dado que ello requiere una base de confianza, es necesario obtener todas las garantías posibles acerca de quién es la persona que está "del otro lado", es decir, poder identificarla digitalmente. De ahí que entiendo que la identidad digital cumple un rol fundamental en el desarrollo del gobierno y del comercio electrónico.

2- ¿Cómo califica usted el estado actual de las técnicas de identidad digital en Uruguay? ¿Qué factores condicionan los avances en la materia?

En Uruguay se cuenta actualmente con diversas formas de identificar a los usuarios de gobierno y comercio electrónico, tanto haciendo uso de usuarios y contraseñas, sistemas de One-time Password, certificados digitales y biometría. El factor clave para contar con sistemas de identificación digital es contar con aplicaciones de uso masivo que la utilicen. De nada me sirve tener una identidad digital si no tengo dónde usarla.

3.- ¿Qué grado de interés manifiestan actualmente la comunidad uruguaya por la cuestión de la identidad digital?

Tanto el gobierno como el sector financiero están trabajando fuertemente en el desarrollo de distintas técnicas que permitan identificar de forma digital a personas y empresas con el propósito de poder realizar transacciones de forma confiable y segura.

4.- ¿Qué iniciativas de identidad digital existen en Uruguay?

Como se mencionó anteriormente, en Uruguay existen variedad de formas de identificación digital. Por otro lado, actualmente se esta trabajando en un proyecto piloto para implementar un Documento de Identidad Electrónico, el cual servirá para identificarse ante sistemas TIC, de manera análoga a como lo hace el documento de identidad en el mundo físico. Para esto, fue necesario realizar cambios normativos que reconozcan el uso de tecnologías como la firma electrónica, analizar las soluciones tecnológicas disponibles y aprender de otros países que ya hayan realizado este tipo de actividades. Particularmente, el proyecto se implementará entre 2013 y 2014.

5.- ¿Cuál es el potencial previsible de las herramientas de e-Gobierno y de las TIC en materia de identidad digital y biometría?

Así como la identificación de personas es fundamental en el mundo físico, lo es en el mundo virtual. Es allí donde la identificación electrónica se constituye en un factor clave para el desarrollo de comercio y gobierno electrónico. El potencial es enorme, teniendo en cuenta el desarrollo de las TIC en general, pero particularmente en gobierno y comercio electrónico. Es un tema de confianza. No sería posible realizar transacciones electrónicas si no contáramos con métodos de identificación electrónica confiables y seguros.

RESEÑA BIOGRÁFICA DE LOS ENTREVISTADOS

Steven Griner, OEA

Coordinador del Programa de Universalización de la Identidad Civil en las Américas de la OEA (PUICA). Comenzó su trayectoria en la OEA en 1993, como funcionario de la Unidad para la Promoción de la Democracia, coordinando el Programa Especial de la OEA para el Apoyo al Proceso de Paz en Guatemala y el Foro Interamericano sobre Partidos Políticos, entre otras responsabilidades. Entre 2006 y 2011 sirvió como jefe de la Sección de Observación Electoral, habiendo observado más de 50 elecciones en America Latina, el Caribe, África y Asia Central. Sirvió como voluntario del Cuerpo de Paz en Guatemala y trabajó en el Instituto Nacional Demócrata para Asuntos Internacionales en Washington, D.C. Tiene títulos académicos en Lenguas Modernas y Administración de Empresas de Texas A&M University y una maestría del Johns Hopkins School of Advanced International Studies (SAIS).

Ramón Gerónimo Brenna, Argentina

Profesor de Posgrado en el Programa de Actualización en Derecho Informático On Line, de la Facultad de Derecho de la Universidad de Buenos Aires, desde 2000 a la fecha. Director de los Equipos Técnicos del "Digesto Jurídico Argentino" y de diversos Digestos Provinciales, Presidente de ARGENJUS, Presidente alterno de la Mesa Permanente de Justicia del Diálogo Argentino. Coordinador del Instituto Internacional de Estudios y Formación sobre Gobierno y Sociedad -IIEFGS- Universidad del Salvador- Universitá di Pisa Italia. Profesor titular de diversas carreras de grado y postgrado. Autor de numerosos trabajos y publicaciones en el país y en el exterior. Representante argentino en distintos congresos y jornadas nacionales y extranjeras. Es Abogado graduado con diploma de honor en la Universidad de Buenos Aires y Magíster en Ciencia de la Legislación (Universidad de Pisa, Italia).

César López, Perú

Ejecutivo Senior con experiencia en gerencia y planeamiento estratégico institucional basado en el uso y gobierno corporativo de TIC. Es especialista en temas de gestión de identidad, biometría y definición de soluciones innovadoras para el mejoramiento de procesos y optimización de capacidades operativas, funcionales y de servicios. Actualmente es Director General de Tecnología de Información del Ministerio de la Producción del Perú, estando cargo de proyectos de administración, gestión y monitoreo de políticas de Estado. Es consultor de la empresa Presencia Systems especializada en gestión de identidad y flujos digitales de información. Ha sido CIO del Registro Nacional de Identidad y Estado Civil (RENIEC) durante más de seis años, Jefe de la Oficina Nacional de Gobierno Electrónico de la Presidencia del Consejo de Ministros, Consultor Senior de IBM del Perú en planeamiento estratégico, e-Business y CMMi. Actuó también como Consultor en TIC en proyectos del BID y UN. Es especialista Six Sigma (Programa Champion), es licenciado en Investigación Operativa, cuenta con un MBA, desarrolló cursos de e-Gobierno en Seúl, Corea, y cursos de administración de e-Gobierno en OEA Actualmente cursa el Doctorado en Dirección Estratégica de Empresas, en Maastricht Management School / CENTRUM.

Santiago Paz, Uruguay

Director y fundador del Centro Nacional de Respuesta a Incidentes de Seguridad Informática de Uruguay (CERTuy). Ha estado a cargo de diversos proyectos de tecnología para el gobierno de Uruguay, entre los que se estacan: implementación de la red privada del gobierno, diseño e implementación de los sistemas de seguridad de la plataforma de Gobierno Electrónico, e Infraestructura Nacional de Clave Pública de Uruguay. Cuenta con más de 10 años de experiencia en la industria, habiendo desarrollado proyectos para el sector privado en Uruguay, Ghana, Pakistán, Puerto Rico y Belice. Es coautor del libro Wireless Engineering Body of Knowledge de IEEE, fue directivo del capítulo Uruguay de IEEE, docente universitario desde 2004 en la Universidad ORT de Uruguay y autor de varios artículos referidos a TIC. Es Ingeniero en Telecomunicaciones especializado en Seguridad Informática. Está certificado como auditor de sistemas por ISACA (CISA), como practitioner en seguridad informática por ISC2 (SSCP) y como gerente de proyectos por el PMI (PMP).

EN ESTE NÚMERO

Curso OEA Aspectos Regulatorios del Gobierno Electrónico

La OEA ofrece el curso en línea de Aspectos Regulatorios del Gobierno Electrónico, cuyas ocho ediciones –hasta la fecha- han sido altamente calificadas.

La SAP/OEA ofrece, en su Campus Virtual, el Curso de Aspectos Regulatorios del Gobierno Electrónico (*) del cual se dictaron ocho (8) ediciones que resultaron altamente valoradas por sus egresados y por las organizaciones en que éstos se desempeñan.

El Curso fue diseñado y desarrollado por los especialistas Erick Iriarte Ahon, Fernando Maresca y María Clara Gutiérrez. Esta última profesional es quien coordina, en la actualidad, las sucesivas ediciones.

Destinatarios

El curso está dirigido a gerentes públicos y personas con puestos directivos en la administración pública, así como a profesionales, académicos y estudiantes interesados en utilizar la normatividad TIC como herramienta para mejorar la gestión de gobierno.

Objetivos y resultados previstos

El objetivo del curso es que los participantes conozcan y comprendan los principios y aspectos legales relacionados con el diseño e implementación de estrategias de e-Gobierno, a través de una visión global y de un análisis focalizado de la normatividad y de experiencias exitosas en el desarrollo e implementación de proyectos en la materia.

Al finalizar el curso los participantes están calificados con conocimientos sobre los aspectos regulatorios necesarios para lograr un avance sostenido de las iniciativas de e-Gobierno, el marco regulatorio internacional del e-Gobierno, así como algunos modelos de referencia que podrán utilizar para regular el e-Gobierno en su propio entorno.

Mediante la aplicación de los lineamientos provistos, adaptados a cada caso específico, los participantes identifican necesidades a satisfacer en sus instituciones, las abordan teniendo en consideración los elementos críticos en la planificación de los marcos normativos y formulan un proyecto relacionado con una iniciativa puntual que facilite el abordaje de la estrategia en su entidad.

Programa

El curso se dicta completamente en línea durante 8 semanas. Cada semana se desarrolla un módulo, a través de lecturas, intercambios y actividades en línea, que los participantes pueden realizar en sus propios tiempos, sin horarios fijos de conexión. A través del aula virtual, el cursante participa en foros interactivos, actividades y chats coordinados por tutores especializados, quienes lo asisten, orientan y retroalimentan, permitiéndoles asumir un rol activo en el proceso de aprendizaje. Como parte del curso cada participante elabora un trabajo final cuyo objetivo es la puesta en práctica de los conocimientos mediante la elaboración de una propuesta de proyecto que esté relacionado con su entorno laboral.

Se inicia con el Módulo 0 -"Para Comenzar"- destinado a adquirir los conocimientos y habilidades necesarias para un correcto manejo del Aula Virtual y sus herramientas, seguido de 7 módulos de contenidos y 1 de cierre y evaluación final. Los temas principales de cada módulo semanal se detallan a continuación:

Semana 1: Módulo 0: Para comenzar, bienvenida, socialización y uso de las herramientas del aula. Módulo 1: Regulación en el marco de las políticas de la Sociedad de la Información (Parte I).

Semana 2: Módulo 2: La regulación en el marco de las políticas de la Sociedad de la Información (parte II).

Semana 3: Módulo 3: Regulación de e-Gobierno: Marco conceptual**.**

Semana 4: Módulo 4: Transacciones y Regulación en e-Gobierno

Semana 5: Módulo 5: Seguridad de la Información

Semana 6: Módulo 6: Privacidad y otros aspectos clave de la regulación del e-Gobierno.

Semana 7: Módulo 7: Regulación y e-Democracia

Semana 8: Módulo de Cierre: Proyecto Final de Evaluación

Próxima edición: Edición 10, Abril 2013

(*) Desarrollado con apoyo del IDRC y del BID.

USTEDES LO ESTÁN HACIENDO

Conferencia internacional de privacidad de datos

Con más de 90 expositores, representando a 40 países, finalizó con éxito la 34 Conferencia de Autoridades de Control de Datos Personales realizada en Uruguay. En el cierre, el director de AGESIC José Clastornik señaló que más importante que las respuestas son los interrogantes, en ese equilibrio entre la innovación y los derechos de las personas.

Más información: http://www.redgealc.net/con-equilibrio-finalizo-privacy-conference-2012/contenido/5220/es/

Perú invertirá U$D 420 millones para la red de fibra óptica

En el marco de la decisión de promover la implementación de fibra óptica a nivel nacional, Perú prevé invertir 420 millones de dólares para la red dorsal de fibra óptica en el año 2013. Con ello, los usuarios finales, aun quienes residen en lugares remotos del país, podrán acceder a la red de telecomunicaciones con velocidades altas para aplicarlo en el campo de la medicina, educación y seguridad nacional, así como otros usos.

Más datos: http://www.redgealc.net/el-gobierno-invertira-420-millones-de-dolares-para-la-red-de-fibra-optica/contenido/5205/es/

Modernizan sistema para buscar empleo en El Salvador

El sistema de intermediación laboral, que administra el Ministerio de Trabajo y Previsión Social, fue modernizado recientemente para ofrecer un mejor servicio digitalizado sobre los puestos de trabajo que ofrece tanto el sector privado como el público.

Más datos: http://www.redgealc.net/ministerio-de-trabajo-modernizan-sistema-para-buscar-empleo-en-el-salvador/contenido/5226/es/

Colombia: Foro Mundial Contra el Hurto de Celulares

El Gobierno de Colombia, junto con la Cámara Colombiana de Informática y Telecomunicaciones CCIT y la Policía Nacional de Colombia, llevó a cabo el Gran Foro Mundial Contra el Hurto de Celulares, con el propósito de adoptar medidas conjuntas para enfrentar la creciente problemática de la compraventa ilícita de móviles.

Más datos en: http://www.redgealc.net/foro-mundial-contra-el-hurto-de-celulares/evento/245/es/

PARA TENER EN CUENTA

1.- La usurpación de identidad

Amparado por el anonimato que ofrecen las redes sociales y los trámites online, el delito de usurpación de identidad se difunde aceleradamente. La acción de adoptar deliberadamente la identidad de otra persona para realizar actos fraudulentos comerciales, civiles o penales, acceder a cuentas bancarias o cometer delitos es cada vez más fácil y frecuente.

Según un sondeo realizado y publicado en Francia, por el instituto CSA:

- El 8% de los franceses declaran haber sido víctimas de usurpación de identidad en los últimos 10 años, mientras que sólo el 4,2% lo señalaban en 2009.

- El 63% de los franceses perciben alto riesgo de ser víctimas de delitos de identidad.

Si bien se prevé que la utilización de técnicas biométricas y la inserción de chips en los documentos de identidad reducirán una parte del riesgo, aún no se dispone de soluciones eficaces para prevenir la usurpación de identidad en redes sociales, una práctica cada vez más común que pone en riesgo la seguridad de la víctima y su propia reputación.

Fuente: CSA: Les Français et la criminalité identitaire. Sondage de l'Institut CSA. Conférence de presse du 10 octobre 2012

http://www.csa.eu/multimedia/data/sondages/data2012/opi20120830-Les-francais-et-la-criminalite-identitaire.pdf

2.- CIBRA2012 - Congreso Internacional de Biometría de la República Argentina

Durante los días 5 y 6 de noviembre se realizó en Buenos Aires el 7º Congreso Internacional de Biometría de la República Argentina denominado CIBRA2012, con el objetivo de continuar las tareas de difusión del uso, las aplicaciones y los proyectos con herramientas biométricas. Los principales temas tratados por los expositores nacionales e internacionales estuvieron referidos a experiencias nacionales, estándares, privacidad, marco legal y aplicaciones en servicios de identificación, sociales, electorales y de seguridad. Se repasaron diversas aplicaciones biométricas en distintos niveles del Estado; por ejemplo, la identificación de niños recién nacidos en hospitales mediante huellas digitales de manos, pies y fotos del rostro, los registros de ingreso/egreso de pasajeros mediante sistemas biométricos en puestos migratorios. Se trata de actualizaciones y mejoras en servicios que impactan en la calidad de vida y la seguridad de los ciudadanos. La participación de expositores de EE.UU., Estonia Francia, Honduras, India, Inglaterra, Irlanda, México y Portugal, permitió delinear un panorama de lo que sucede en distintas latitudes.

3.- Recensión: preguntas frecuentes sobre biometría

La presentación de Preguntas Frecuentes fue desarrollada por el Consejo Nacional de Ciencia y Tecnología (NSTC) de EE.UU. y su Subcomité de Biometría (NSTC Subcommittee on Biometrics). Las respuestas están destinadas a una audiencia general y en ningún caso reemplazan fuentes más descriptivas y precisas en sus aspectos técnicos.

i. ¿Qué es la biometría?: Biometría es un término utilizado alternativamente para describir: (a) una característica biológica o de comportamiento que se puede medir y representar para el reconocimiento automático, o (b) un método automático de reconocimiento de individuos, basado en características biológicas y de comportamiento medibles.

ii. ¿Cuáles son las técnicas biométricas más comunes?: Las huellas dactilares, rostro, iris, voz, firma y geometría de la mano, hallándose muchas otras modalidades en distintas etapas de desarrollo y evolución.

iii. ¿Cómo se recogen los datos biométricos?: Mediante sensores que recolectan y digitalizan los datos necesarios para el reconocimiento; por ejemplo, cámaras digitales para reconocimiento facial o un teléfono para reconocimiento por voz.

iv. ¿Cómo operan los sistemas biométricos?: Mediante un proceso de tres pasos: (a) recopilación de los datos biométricos mediante sensores, (b) conversión a una representación digital denominada plantilla biométrica (template), y (c) comparación de la planilla confeccionada con plantillas almacenadas en la base de datos, lo que resulta en una coincidencia o una incompatibilidad, y las acciones pertinentes (permitir el acceso, activar una alarma, etc).

v. ¿Cuáles son los componentes de un sistema biométrico?: Un sistema biométrico típico contiene cinco componentes integrados: (a) un sensor que reúne los datos y los convierte a formato digital, (b) los algoritmos de procesamiento de la señal que controlan la calidad del registro y desarrollan la plantilla biométrica (template), (c) un componente de almacenamiento de la base de datos, (d) un algoritmo de coincidencias que compara la plantilla biométrica de la muestra con las almacenadas en la base de datos, y (e) un algoritmo de decisión (automatizada o con asistencia humana) que utiliza los resultados del componente de coincidencias para determinar la coincidencia o la incompatibilidad.

vi. ¿Cuál es la diferencia entre verificación e identificación?: En la verificación el sistema biométrico intenta confirmar la identidad proclamada de un individuo mediante la comparación de una muestra con registros almacenados previamente. En la identificación el sistema intenta determinar la identidad de un individuo comparando su registro biométrico contra todos los existentes en la base de datos.

vii. ¿Cuándo es necesario un sistema biométrico?: Para determinar si es necesario un sistema biométrico, deben estar claros los requerimientos operacionales y las condiciones ambientales de cada caso. Dado que la biometría es un componente de la arquitectura de un sistema global, no debe ser forzada, debiendo evaluarse cada circunstancia para determinar un balance entre los beneficios y costos de un sistema biométrico. .

viii. ¿Cómo seleccionar una tecnología biométrica?: La efectividad de una tecnología biométrica depende de cómo y dónde se la utiliza. Cada modalidad biométrica tiene sus fortalezas y debilidades que deben ser evaluadas en relación con la aplicación. Algunos factores clave son: evaluación del ambiente, necesidades de rendimiento, tamaño de la población, la demografía y ergonomía, la interoperabilidad con otros sistemas existentes, consideraciones de usuario, etc.

Fuente:http://www.biometria.gov.ar/acerca-de-la-biometria/preguntas-frecuentes.aspx

NOTICIAS

El Campus Virtual de la Secretaría de Asuntos Políticos (SAP) de la OEA está incorporando un conjunto de nuevas actividades de notoria significación para la región, entre las cuales destacamos las siguientes: a) Curso Gestión de las Compras Públicas, (b) Curso Gestión de las Compras Públicas, edición especial para Haití, (c) Curso Gestión de las Compras Públicas edición especial para la Red Interamericana de Compras Gubernamentales, y (d) Nuevo Modelo de Gobierno En Línea: Evolución y Contexto.

A continuación sintetizamos algunas características de dichos cursos, los cuales se están impartiendo en línea con satisfactorios niveles de participación:

(a) Curso Gestión de las Compras Públicas

El objetivo del curso es el desarrollo profesional de funcionarios que desempeñan funciones vinculadas a la compra y contratación de obras, bienes y servicios gubernamentales, a través del uso de conceptos, métodos y mejores prácticas para una gestión efectiva. Se tratan los fundamentos, procesos y gestión de las compras públicas en diversos entornos y situaciones, así como el aprovechamiento de las TIC en la gestión.

(b) Curso Gestión de las Compras Públicas 2ª edición especial para Haití

Esta edición especial -en idioma francés- se desarrolla a través del esfuerzo conjunto de la OEA y del BID, dentro de las actividades de apoyo de ambas instituciones al proceso de modernización institucional de Haití, Una primera etapa se concretó entre julio y septiembre, desarrollándose actualmente la segunda etapa. Se está capacitando a más de 300 funcionarios con contenidos específicos vinculados a las peculiares características de este país.

(c) Curso Gestión de las Compras Públicas 10ª edición especial para la Red Interamericana de Compras Gubernamentales.

Este curso forma parte de la contribución del Departamento para la Gestión Pública Efectiva (DGPE) de la SAP de la OEA a la Red Interamericana de Compras Gubernamentales (RICG).

(d) Nuevo Curso Especial Colombia: "Modelo de Gobierno en Línea: Evolución y Contexto"

Este curso es el resultado del trabajo mancomunado que viene realizando el Ministerio de las Tecnologías de la Información y las Comunicaciones -MinTIC- del Gobierno de Colombia, a través de su iniciativa "Prepárese" y la SAP de la OEA en su misión de promover la eficacia y la transparencia en la gestión gubernamental.

En el año 2011 el MinTIC y la SAP de la OEA impartieron el curso "Gobierno en Línea: Evolución y contexto de la estrategia" con el propósito de lograr una compenetración de los funcionarios con la evolución de la Estrategia de Gobierno en Línea –GEL- y sus oportunidades, fortalezas y retos para las entidades, los servidores y la ciudadanía. Se procuró asimismo incentivar la gestión e innovación en el planteamiento de soluciones de GEL centradas en los procesos y con participación de la ciudadanía; identificar proyectos transversales, estratégicos y multidimensionales, analizar las recomendaciones y lineamientos del Manual de Gobierno en Línea, así como proyectar iniciativas de autoevaluación, monitoreo y seguimiento para realimentar la evolución en el Modelo. Dicho curso se dirigió a 260 servidores públicos del Orden Nacional, interesados e involucrados en la implementación de la Estrategia GEL en sus entidades.

Dando continuidad a ese camino, el nuevo curso tiene por objetivo que los participantes adquieran los conocimientos para garantizar el máximo aprovechamiento de las TIC en el marco de un Gobierno Abierto que contribuya a la construcción de un Estado más eficiente, transparente y participativo y que preste mejores servicios con la colaboración de toda la sociedad. En la primera edición participaron más de 220 funcionarios, previéndose una segunda edición con similar cantidad de participantes.

Los temas que se tratan son: La estrategia GEL, sus componentes y su articulación con los planes nacionales; planeación, monitoreo, evaluación y avance; habilitadores de GEL; inicio del nuevo modelo; componentes de elementos transversales; componentes de Información, Interacción, transacción y democracia en línea; consejos para la implementación de la estrategia.

ENLACES

Enlaces recomendados a los interesados en la temática **e-Gobierno, Gestión de Identidades y Biometría**

Ágora SIC: El iris ocular como parámetro para la identificación Biométrica

http://www.revistasic.com/revista41/pdf_41/SIC_41_agora.PDF

Argentina. Biometría

http://www.biometria.gov.ar/

Argentina. Biometría. Preguntas frecuentes

http://www.biometria.gov.ar/acerca-de-la-biometria/preguntas-frecuentes.aspx

Australia implementa biometría para combatir fraude en trámites de visa

http://www.dailytelegraph.com.au/news/biometric-security-at-borders-to-catch-visa-fraud/story-e6freuy9-1226315240076

Bath University Iris Image Database

http://www.smartsensors.co.uk/information/bath-iris-image-database/

Biometric Consortium

http://www.biometrics.org/

Centro Virtual Cervantes (España): Proyecto de una base de datos acústicos de la lengua española. Joaquim Llisterri, Dolors Poch. Universidad Autónoma de Barcelona

http://cvc.cervantes.es/obref/congresos/sevilla/tecnologias/ponenc_llisterripoch.htm

Chile. Gobierno Regional de Valparaíso: Aprueba la política institucional sobre control de acceso

http://www.gorevalparaiso.cl/descargas/PMG2011/20111228174540463.pdf

Ecuador. Proceso de Implementación del Sistema de Autenticación Biométrica

http://www.finanzas.gob.ec/?p=3219/proceso-de-implementacion-del-sistema-de-autenticacion-biometrica

EE.UU. (USA). Biometric portal. National Institute of Standards and Technology (NIST). U.S. Department of Commerce.

http://www.nist.gov/biometrics-portal.cfm

EE.UU. (USA). Biometrics.gov Estándares biométricos

http://www.biometrics.gov/Standards/Default.aspx

EE.UU. (USA). Department of Commerce. NIST: Iris Challenge Evaluation: a contest for competing iris-recognition algorithms. The National Institute of Standards and Technology (NIST)

http://www.nist.gov/itl/iad/ig/ice.cfm

EE.UU. (USA). Department of Defense: Biometrics Identity Management Agency

http://www.biometrics.dod.mil/

EE.UU. (USA). FBI. Biometric Center of Excellence (BCOE)

http://www.biometriccoe.gov/

España. IRIS-CERT. Autenticación de usuarios

http://www.rediris.es/cert/doc/unixsec/node14.html

ISO/IEC: ISO/IEC 19794-6 International standard for iris images

http://www.iso.org/iso/catalogue_detail.htm?csnumber=38750

ISOC-AR: Biometría y Privacidad.

http://www.isoc.org.ar/proyectos/Brenna.ppt

ITU. Biometría y normas. Informe Technology Watch

http://www.itu.int/net/itunews/issues/2010/01/05-es.aspx

ITU: Biometrics and Standards. ITU-T Technology Watch Report December 2009

http://www.itu.int/dms_pub/itu-t/oth/23/01/T230100000D0002PDFE.pdf

John G. Daugman's original patent application at Google Patents. World largest current deployment

http://www.google.com/patents?id=KRkpAAAAEBAJ

Project Iris (Reino Unido): Project Iris an Open Source iris recognition system

http://projectiris.co.uk/

Real Instituto Elcano (España): Control biométrico: el necesario debate público (ARI). James Ross.

http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/defensa+y+seguridad/ari+154-2003

Sistemas de autenticación biométricos: seguridad y protección de la Información. Ricardo Llopis Nebot

http://spi1.nisu.org/recop/al01/llopis/Biometricos.PDF

Sistemas de identificación biométrica mediante patrón de iris utilizando representación multi-escala e información de fase

http://www.criptored.upm.es/guiateoria/gt_m279a.htm

Sociedad Española de Biometría

http://www.biometricsociety.net/

Speech Recognition HOWTO. Stephen Cook

http://www.tldp.org/HOWTO/Speech-Recognition-HOWTO/

Speech Synthesis & Analysis Software

http://linux-sound.org/speech.html

Universidad Central de Venezuela. Escuela de Ingeniería: Sensores biométricos

http://neutron.ing.ucv.ve/revista-e/No6/Olguin%20Patricio/SEN_BIOMETRICOS.html

Universidad Nacional de la Plata (Argentina). Servicio de Difusión de la Creación Intelectual (SeDiCI): Los sistemas biométricos y su factibilidad de aplicación en organismos estatales

http://sedici.unlp.edu.ar/bitstream/handle/10915/19487/Documento_completo.pdf?sequence=1

Universidad de la República (Uruguay). Facultad de Ingeniería: Control de calidad en imágenes de iris mediante razonamiento ontológico

http://www.fing.edu.uy/inco/eventos/cibsi09/docs/Papers/CIBSI-Dia3-Sesion9%284%29.pdf

Universidad de la República (Uruguay). Facultad de Ingeniería. Instituto de Ingeniería Eléctrica (IIE): Reconocimiento de iris para el MATLAB

http://iie.fing.edu.uy/investigacion/grupos/gti/timag/trabajos/2004/recon_iris/prog/prog.htm

Universidad Politécnica de Madrid (España). Área de Tratamiento de Voz y Señales. Laboratorio de Identificación Biométrica: Modalidades en los Sistemas de Autenticación Biométrica

http://gavab.escet.urjc.es/recursos/JOrtega04.pdf

Universidad Politécnica de Madrid (España). Centro de Difusión de Tecnologías (CEDITEC): Seguridad y Biometría en el Móvil

http://www.ceditec.etsit.upm.es/index.php?option=com_content&view=article&id=21670&Itemid=1371&lang=es

University of Cambridge (Reino Unido). Computer Laboratory: United Arab Emirates Deployment of Iris Recognition

http://www.cl.cam.ac.uk/~jgd1000/deployments.html

Nota: Invitamos a todos los lectores a sugerirnos la inclusión de recursos y a avisarnos en caso de que alguno de los vínculos publicados se hallara dañado. Con esta colaboración podremos ofrecer un mejor material. Dirigir sus sugerencias y avisos a: Javier Sáenz Coré <jsaenz@oas.org>

(*) El correcto funcionamiento de los URL indicados en cada una de las referencias de esta sección fue verificado entre los días 26 y 31/10/2012.