



108

EDICIÓN

Boletín e-Gobierno Red GEALC

OCTUBRE 2015



“e-Gobierno y autenticación de identidad”

TABLA DE CONTENIDO

▪ REFLEXIÓN	2
▪ ENFOQUES Y TENDENCIAS	3
▪ NOVEDADES	10
▪ REFERENCIAS	15

CRÉDITOS

Comité Editorial

María Fernanda Trigo, Directora del Departamento para la Gestión Pública Efectiva, OEA

Mike Mora, OEA

Miguel A. Porrúa, Especialista Líder en e-Gobierno, BID

Roberto López, Gerente Red GEALC

Coordinador del Boletín

José Luis Tesoro

Publicación

Marcela Petrovic

REFLEXIÓN

Una de las cuestiones que condicionan 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 gestionar lo que solicita.

La identidad está constituida por el conjunto de rasgos propios que caracterizan a una persona en relación a las demás (nombre y apellido, sexo, filiación, nacionalidad, fecha de nacimiento, domicilio, teléfono, número de documento personal, estado civil, patrones biométricos, entre otros). La notoria evolución de las técnicas biométricas permite alcanzar crecientes niveles de confiabilidad, mediante el reconocimiento de huellas dactilares, patrones faciales, palmares, de voz, oculares o de ADN, así como de combinaciones multi-biométricas.

Para ser viable, un sistema de autenticación debe ser: (a) fiable en relación al riesgo implicado, (b) económicamente factible, (c) resistente a eventuales ataques, y (d) aceptable para los usuarios. La evidencia empírica muestra que no es sencillo lograr un equilibrio, entre los referidos factores, que promueva el desarrollo y uso del e-Gobierno.

La Red GEALC promueve y facilita el intercambio de experiencias y herramientas TIC dirigidas a flexibilizar los procesos de autenticación mediante la graduación de requisitos en función de los riesgos implicados en cada tipo de trámite o servicio.

En este número del Boletín, referido a “e-Gobierno y autenticación de identidad” presentamos entrevistas con autoridades de Chile y de Estonia competentes en la materia, así como documentos y notas pertinentes. Confiamos en que su disseminación contribuya a promover la racionalización de los procesos de autenticación en función de los riesgos implicados en cada caso, en beneficio del desarrollo del e-Gobierno y de nuestras sociedades. Esta temática fue anteriormente abordada en nuestro Boletín N° 79, de noviembre 2012, referido a “e-Gobierno y Gestión de Identidades”.

Red de Gobierno Electrónico de América Latina y el Caribe (Red GEALC)

Organización de los Estados Americanos (OEA), Banco Interamericano de Desarrollo (BID), Centro de Investigación para el Desarrollo Internacional (IDRC)

ENFOQUES Y TENDENCIAS**“e-Gobierno y autenticación de identidad”**

Entrevista con Jorge Alzamora Contreras, Jefe de División de la Unidad de Modernización del Estado y Gobierno Digital, Ministerio Secretaría General de la Presidencia, República de Chile.



Por José Luis Tesoro

1.- ¿Cómo visualiza la cuestión de la autenticación de identidad en materia de e-Gobierno?

La autenticación de la identidad de las personas es un habilitante para el e-Gobierno, ya que - por ejemplo- permite al Estado personalizar la prestación de servicios de acuerdo con el perfil de cada usuario.

La tecnología actualmente disponible no es costosa, y su impulso es decisión de cada gobierno. Sin embargo, para que su uso y masificación sean efectivos en términos del impacto esperado, es fundamental que el sistema adoptado garantice una adecuada protección de datos y genere plena confianza, tanto en las personas como en las instituciones.

2.- ¿En qué grado percibe que la masificación del e-Gobierno resulta limitada por la complejidad de las modalidades “seguras” de autenticación de identidad?

El equilibrio entre difusión y seguridad es un desafío propio de cualquier proyecto tecnológico. Para que el uso de “tecnologías seguras” no obstaculice la difusión, debemos arbitrar los criterios sobre los cuales procuramos sustentar el referido equilibrio.

Tanto para la ciudadanía como para las instituciones es muy relevante que los sistemas informáticos sean seguros, ya que ello se traduce en confianza. Pero no deberían adoptarse estándares de seguridad tan altos o complejos que obstaculicen o bloqueen el uso de los sistemas. Otro factor determinante de la factibilidad de masificar el uso de sistemas es la facilidad de uso.

3.- ¿Cuáles son, a su criterio, los factores que limitan la difusión masiva de la firma electrónica en e-Gobierno?

La implementación de la firma electrónica se ha visto como un fin en sí mismo, sin tener en cuenta que la relevancia de una tecnología depende primordialmente del papel que se le asigne en una cadena de valor.

La firma electrónica es una tecnología habilitante valiosa dentro de un proceso de gestión documental que genere valor para el ciudadano, en el marco de una gestión pública con altos niveles de eficacia y eficiencia.

En el caso chileno, existe una ley desde el año 2002, cuyo foco ha estado en la forma de uso de la tecnología y no en la generación de casos de uso que la hacen valiosa. Por eso estamos implementando la firma electrónica avanzada con nuestros ministros, subsecretarios y altos directivos del Estado. Es un esfuerzo de largo aliento, cuyo objetivo final es expandir su uso a otros niveles.

4.- ¿Cómo distinguiría usted los trámites de e-Gobierno para ponderar el nivel de seguridad requerido en la autenticación de identidad?

Los trámites informativos u otros similares que operan con datos públicos no requieren altos niveles de seguridad. Cuando se opera con datos personales e información sensible (por ejemplo: historias clínicas), deben exigirse los máximos niveles de seguridad y autenticación. En el caso chileno, por ejemplo, no es lo mismo autenticar una solicitud de certificado de nacimiento, que contiene información pública y notoria, que autenticar una solicitud de certificado de antecedentes, que contiene información personal más sensible.

5.- ¿Podría proporcionarnos sus comentarios acerca de la experiencia de Chile en materia de graduación de requisitos de autenticación en función de la sensibilidad, vulnerabilidad y nivel de riesgo?

En materia de mecanismos de autenticación eficaces, la experiencia de la banca chilena ha sido exitosa, pues cada operación vía internet requiere superar dos o más instancias de identificación.

En el Estado, la implementación de la firma electrónica avanzada con nuestros ministros, subsecretarios y altos directivos contempla diversos niveles de autenticación. En concreto, contamos con un sistema encriptado llamado FED, que centraliza y protege las firmas de las autoridades. Para ingresar al FED, es necesario que las autoridades utilicen su Clave Única, que obtienen de manera presencial en el Servicio de Registro Civil e Identificación. Luego, para firmar electrónicamente, se requiere ingresar una contraseña de un solo uso (como la utilizada por los bancos).

6.- ¿Cuáles son las experiencias más efectivas de Chile en materia de autenticación transfronteriza de identidad?

Actualmente Chile es parte del sistema Visa Waiver, que permite ingresar a Estados Unidos por vía de una autenticación electrónica de identidad que opera en reemplazo de la tradicional visa. Este sistema ha resultado efectivo para los viajeros, e incluso abrió la posibilidad de ingresar a Canadá. En nuestra región, ello requiere de acuerdos y protocolos entre los países.

Por otra parte, en esta materia cabe resaltar una discusión —aún incipiente— en el marco de la Red GEALC, donde se está hablando de la homologación de los certificados raíces como un mecanismo que, a la vez, ayude a impulsar la firma electrónica en los países.

7.- ¿Desea agregar algún comentario adicional?

Deseo insistir en que los gobiernos debemos distinguir y hacer claramente visible la relevancia de las herramientas que utilizamos dentro de las cadenas de valor de los procesos, tanto de gestión interna como de gestión de cara al ciudadano.

Por ejemplo, la firma electrónica es una herramienta fundamental para la homologación funcional de los documentos electrónicos, lo que se traduce en gestión documental efectiva, con menos burocracia.

En nuestra experiencia, sólo recientemente los proveedores están percibiendo que los certificados de firma no son -en sí- generadores de valor en la gestión, sino sólo habilitadores. Por esto, para generar propuestas efectivamente valiosas para el Estado y los ciudadanos, es necesario establecer los casos de uso, los aportes a las cadenas de valor y sus distintos eslabones, así como los actores involucrados.

Jorge Alzamora Contreras

Es Jefe de División de la Unidad de Modernización del Estado y Gobierno Digital, del Ministerio Secretaría General de la Presidencia de la República de Chile. En su desempeño profesional ha sido Administrador Municipal de la Municipalidad de Maipú; Jefe del área Legislativa e Internacional del Instituto Nacional de la Propiedad Industrial; Director de Gestión de Investigación, Desarrollo e Innovación del Instituto de Innovación en Minería y Metalurgia S.A. filial de Codelco; y Director del Área de Innovación y Transferencia de Tecnología del Estudio Albagli y Zaliasnik. En su desempeño académico ha sido profesor de distintas ramas del Derecho en la Universidad Andrés Bello, Miguel de Cervantes, San Sebastián y Adolfo Ibáñez. Es abogado de la Pontificia Universidad Católica de Chile, con un Máster en Derecho de las Tecnologías de la Universidad de Ottawa, Canadá.

Entrevista con Liina Areng, Directora de Relaciones Internacionales de la Autoridad Nacional del Sistema de Información de Estonia



Por Mike Mora

[Enlace al texto en inglés](#)

1.- ¿Cómo visualiza hoy la cuestión de la autenticación de identidad en materia de e-Gobierno?

Con la creciente difusión de la banca y de otros servicios comerciales vía Internet (m-Parking, Uber, Airbnb, etc.), se manifiesta en la población una creciente expectativa de que los servicios gubernamentales adopten también dicha vía. Los gobiernos están optando por distintos métodos de autenticación electrónica; desde contraseñas y tarjetas inteligentes hasta diversas modalidades biométricas. Tales métodos varían en los niveles de seguridad, usabilidad e interoperabilidad. Estonia ha optado por la autenticación de múltiples capas (Identificación electrónica nacional con PIN), considerando que es la forma más segura de ofrecer a nuestros ciudadanos el acceso a la totalidad de e-servicios públicos y privados.

2.- ¿En qué medida percibe usted que la expansión del e-Gobierno resulta limitada por la complejidad de las modalidades “seguras” de autenticación de identidad?

La expansión del e-Gobierno depende primordialmente de la medida en que éste se desarrolla como habilitador del cambio para facilitar la administración del gobierno, el desarrollo económico y el bienestar social. En Estonia comenzamos a digitalizar los servicios gubernamentales a mediados de la década de 1990, y hoy vemos niveles sustanciales y sostenibles de rentabilidad y viabilidad de estas decisiones, debido al alto número de servicios electrónicos populares que facilitan la vida de las personas ayudándolas a ahorrar tiempo y dinero.

Los e-servicios deben ser accesibles y fáciles de usar y las personas deben experimentar confianza al usarlos. Las cuestiones de privacidad y seguridad de los datos han adquirido una notable relevancia en las relaciones entre el Estado y los ciudadanos. Y ello es razonable, ya que el usuario, al identificarse electrónicamente, entrega más información que en los esquemas de identificación no digital. Pero viéndolo desde una perspectiva distinta, la "trazabilidad" que permite la identificación electrónica puede ser beneficiosa para el usuario, ya que las transacciones del gobierno con los datos de los ciudadanos son también trazables y auditables. Visto desde esa perspectiva de "Gran Hermano revertido", se está añadiendo una importante capa de transparencia que ayuda a generar confianza, que es la piedra angular del éxito del e-Gobierno. En Estonia, hemos reducido al mínimo las inquietudes por la privacidad al proporcionar a los ciudadanos una clara visión acerca de quién ve sus datos (al loguearse en el Portal del Estado usando la identificación electrónica puede ver el registro de sus datos personales) y la posibilidad de restringir el acceso a los mismos.

La identificación electrónica es sólo uno de los elementos fundacionales de un "ecosistema" seguro de e-Gobierno. El otro elemento importante para el desarrollo de un e-Gobierno exitoso es un entorno tecnológico compartido que permita a los diferentes proveedores de servicios (públicos y privados) cooperar entre sí para facilitar la reutilización de los datos y para desarrollar servicios integrados en línea. La solución de Estonia a esta cuestión fundamental fue desarrollar una capa de intercambio de datos X-Road, una red sistemas de información y de bases de datos conectadas con seguridad, posibilitando así los servicios electrónicos integrados. También debe establecerse un marco legal comprensivo para sustentar el uso de soluciones tecnológicas de e-Gobierno. Por ejemplo, cuando en Estonia se desarrolla un nuevo e-servicio público, no se permite diseñar sistemas que almacenen los mismos datos que ya existen en otra base de datos pública.

En suma, todos estos factores (tecnológicos, organizativos y legales) contribuyen a una gestión efectiva de los servicios de e-Gobierno.

3.- ¿Cuáles son, a su criterio, los factores que limitan la difusión masiva de la firma digital en e-Gobierno?

La difusión de las firmas digitales depende ante todo de su usabilidad y de la simplicidad de la plataforma (unos pocos clics, no más). Las personas deben usar su identificación (y los e-servicios) diariamente y percibir claramente sus beneficios.

Una de las razones por la cuales la firma digital no se ha generalizado es porque muy pocas aplicaciones empresariales requieren autenticación de identidad con certificados digitales. Dado que los ciudadanos se comunican con los proveedores privados de e-servicios (como los bancos) con mayor frecuencia que con el gobierno, un modelo de autenticación universal digital concertado con el sector privado ayudaría también a impulsar el uso de los servicios de e-Gobierno.

Para promover la rápida adopción de las firmas digitales y de los e-servicios conectados, el gobierno necesita asociarse efectivamente con el sector privado. En Estonia los bancos fueron los principales impulsores de la identificación electrónica, dado que ésta fue vista como una forma segura y económica para verificar las transacciones bancarias. Los bancos se unieron para promover -con notable éxito- el uso de la identificación electrónica para el público en general.

4.- ¿Podría comentar la experiencia de Estonia en materia de autenticación de identidad?

Estonia está utilizando un método universal de autenticación digital basado en la identificación electrónica nacional. Ello garantiza el máximo nivel de seguridad en todas las transacciones digitales, ya sea en el sector público o en el privado. Un modelo nacional de identificación electrónica es más fácil de manejar y permite ahorrar costos. Además de una mayor seguridad, ofrece también una mayor comodidad para los usuarios, ya que éstos no necesitan memorizar diversas contraseñas ni portar distintas tarjetas inteligentes. Consideramos que la aplicación de esquemas de autenticación con diferentes niveles de seguridad en función de la "criticidad" de los servicios sólo aumenta la complicación y los inconvenientes tanto para los usuarios como para los administradores de sistemas TI, que necesitan adoptar esos diferentes esquemas en sus servicios, complicando la interoperabilidad.

5.- ¿Qué cuestiones particulares involucra la autenticación transfronteriza de identidad y cómo se están abordando en la Unión Europea

La búsqueda de un esquema interoperable para la autenticación electrónica de identidad entre países es fundamental para garantizar la seguridad de los datos y apoyar el e-comercio transfronterizo. Sin embargo, debido a la amplia variedad de métodos de autenticación digital en uso, con diversos niveles de seguridad, ha sido difícil concertar un estándar internacional de identificación electrónica. La regulación eIDAS de la Unión Europea (UE) sobre identificación y confianza para servicios electrónicos, adoptada en 2014, es un paso importante hacia la armonización del marco regulatorio y la creación de un sistema confiable de reconocimiento mutuo e interoperabilidad de múltiples esquemas nacionales de identificación electrónica dentro de la UE. La regulación se sustentó en varios proyectos piloto a gran escala en el ámbito de la UE (STORK, Peppol, EPSOS etc.) que mostraron la factibilidad de lograr la interoperabilidad técnica. Si bien pasará algún tiempo hasta que los 28 Estados miembros adopten plenamente todas las actas de implementación, eIDAS contribuirá eventualmente a impulsar el desarrollo de servicios electrónicos transfronterizos y a facilitar la creación de un Mercado Único Digital de la UE. Si bien ello no será inmediato, confiamos en que será una historia exitosa que alentará a otros países del mundo a seguir el ejemplo.

Liina Areng

Es Directora de Relaciones Internacionales de la Autoridad Nacional del Sistema de Información de Estonia desde marzo de 2014. Anteriormente fue Coordinadora de Asuntos Internacionales del Centro de Excelencia en Ciber-Defensa Cooperativa de la OTAN (OTAN CCD COE). Tiene un título honorario de Embajador de la OTAN CCD COE. Entre 1999 y 2012 ocupó diversas posiciones en el Ministerio de Defensa de Estonia, culminando como Asesor Principal de Ciberseguridad. Entre 2007-2010 se desempeñó como Consejero Asistente de Defensa en la Representación Permanente de Estonia ante la OTAN. Sus posiciones anteriores fueron Asesor en Control de Armas (2005-2007) y Experto Director en Rusia y la Comunidad de Estados Independientes en el Departamento de Política y Planeamiento para la Defensa (2000-2005). Nació en 1977 en Tallin, Estonia, estudió en la Universidad de Oslo (Noruega) y la Universidad de San Petersburgo (Rusia), se graduó en Ciencias Políticas en la Universidad de Tartu y cuenta con una Maestría en Estudios de Paz y Conflicto de la Universidad de Jaume I de España. También trabajó como investigador en el Colegio de Defensa de y la OTAN y participó en varios cursos de formación en servicio en el Colegio de Defensa de Suecia y en la Escuela de la OTAN en Oberammergau.

NOVEDADES

El portal de la Red GEALC (www.redgealc.net) es el más amplio repositorio de documentos y noticias de la región, con actualización diaria, en materia de e-Gobierno. Entre sus noticias de este mes destacamos:

En el ámbito regional

IX Reunión Anual de Red GEALC

Los directores de e-Gobierno de América Latina y el Caribe se reunieron en Ciudad de México el 26 y 27 de octubre para participar de la novena reunión anual desde la fundación de Red GEALC en 2003. Fue la primera vez que lo hicieron con las autoridades electas por los países en 2014 en Cartagena de Indias. Durante la reunión de México se renovaron autoridades, se analizó la ejecución del plan de trabajo 2015 y se elaboró el plan de actividades para 2016. También se realizaron paneles sobre el estado de situación y tendencias de e-Gobierno en la región y en países líderes a nivel global.

Leer más: <http://redgealc.org/todo-listo-para-la-ix-reunion-anual-de-red-gealc/contenido/6436/es/>

Cumbre de la Alianza para el Gobierno Abierto

Inmediatamente después de alojar la IX Reunión Anual de Red GEALC, México fue sede de la Cumbre de la Alianza para el Gobierno Abierto (Open Government Partnership, OGP, en inglés), principalmente en el Palacio de Minería, con 1.500 participantes. Sus jornadas conectan especialmente con las Metas de Desarrollo Sostenible de Naciones Unidas. Varios de los integrantes de Red GEALC extendieron su estadía en México para tomar parte de este evento.

Leer más: <http://ogpsummit.org>

Ganadores excelGOB visitan Corea

Los ganadores de la más reciente edición de los Premios excelGOB, Sistema de información de precios al consumidor (de Uruguay, en la categoría Innovación Social) y Urna de cristal (de Colombia, en la categoría Simplificación de servicios públicos) participaron de una visita técnica a la República de Corea. La visita, como premio obtenido por los ganadores del referido reconocimiento, se concretó entre el 12 y el 16 de octubre de 2015. Como se recordará, la votación y entrega de diplomas se llevó a cabo durante la III Reunión Ministerial de Gobierno Electrónico de América Latina y el Caribe realizada en Colombia el año pasado. Los premios a la excelencia en gobierno electrónico, excelGOB, son convocados cada dos años por la Red GEALC, el BID y la OEA.

Leer más: <http://redgealc.org/ganadores-de-los-premios-excelgob-realizaron-visita-tcnica-a-corea/contenido/6437/es/>

Tercer taller de software público

El 12 y 13 de noviembre se realizará en Tegucigalpa, Honduras, un nuevo taller del Mecanismo Colaborativo Regional de Software Público, que se lleva adelante en el marco de Red GEALC con apoyo del BID. El objetivo principal de esta instancia es discutir un diseño de modelo para avanzar en la comunidad de software público entre los países de la región,

Leer más: <http://redgealc.org/tercer-taller-de-software-publico/contenido/6411/es/>

Datos abiertos, el peso de la evidencia

Hace un año, un grupo de siete investigadores nucleados en la Iniciativa Latinoamericana por los Datos Abiertos (ILDA), como parte de la red OD4D que también integra la Red GEALC, comenzaron a explorar el estado del arte en materia de datos abiertos en América Latina. En ese momento ILDA decidió focalizarse en tres áreas consideradas claves desde la primera Conferencia Regional de Datos Abiertos en 2013 y fueron confirmadas en CONDATOS 2014: ciudades, servicios públicos e instituciones vinculadas a la rendición de cuentas. Ahora ILDA comparte estos estudios como documentos de trabajo (en evolución), para promover un mayor entendimiento y discusión de la agenda de datos abiertos en la región.

Leer más: <http://redgealc.org/los-datos-abiertos-en-america-latina-que-nos-dice-la-evidencia/contenido/6412/es/>

En el ámbito extra-regional

1.- Un relevante ranking internacional: 2015 Waseda- IAC International e-Government Rankings

Fuente: [2015 Waseda - IAC international e-Government ranking survey], June 2015, Tokyo; Japan

Acceso al texto completo:

http://www.e-gov.waseda.ac.jp/pdf/2015_Waseda_IAC_E-Government_Press_Release.pdf

Acceso al resumen

<https://www.waseda.jp/top/en-news/28775>

2015 Waseda-IAC International e-Government Rankings:

<https://www.waseda.jp/top/en-news/28775>

Los rankings internacionales de “e-Gobierno” del Instituto de e-Gobierno de la Universidad de Waseda y la Academia Internacional de CIOs (IAC), son ampliamente reconocidos como referentes en la materia. A continuación transcribimos los resultados de la 11ª edición correspondiente a 2015.

No	Final Rankings	Score	No	Final Rankings	Score	No	Final Rankings	Score
1	Singapore	93.80	22	Thailand	67.31	43	Brunei	51.06
2	USA	93.58	23	Israel	65.80	44	Bahrain	50.50
3	Denmark	91.25	24	HK SAR	65.24	45	Brazil	50.37
4	UK	90.17	25	Malaysia	64.87	46	Argentina	50.32
5	Korea	89.39	26	Portugal	63.93	47	Colombia	49.36
6	Japan	87.77	27	Czech Republic	63.48	48	South Africa	49.30
7	Australia	86.30	28	Italy	61.30	49	China	48.36
8	Estonia	84.87	29	Indonesia	60.11	50	Kazakhstan	47.73
9	Canada	81.45	30	UAE	58.10	51	Saudi Arabia	47.48
10	Norway	79.63	31	Poland	57.30	52	Peru	46.21
11	Sweden	77.95	32	Spain	57.12	53	Tunisia	45.87
12	Austria	77.26	33	Vietnam	57.03	54	Venezuela	44.65
13	New Zealand	76.66	34	Russia	56.56	55	Uruguay	44.01
14	Finland	76.49	35	India	56.42	56	Morocco	43.13
15	Germany	76.46	36	Macau	56.27	57	Pakistan	42.94
16	France	73.39	37	Chile	53.49	58	Costa Rica	42.06
17	Chinese Taipei	72.76	38	Mexico	53.41	59	Georgia	40.73
18	Belgium	71.69	39	Romania	53.11	60	Nigeria	38.37
19	Iceland	69.73	40	Oman	51.60	61	Fiji	37.54
20	Netherlands	69.53	41	Philippines	51.47	62	Egypt	37.19
21	Switzerland	69.17	42	Turkey	51.31	63	Kenya	32.91

Table 1: Waseda – IAC e-Government Overall Ranking 2015

En las encuestas y rankings de “e-Gobierno” elaborados por Waseda - IAC se evalúa –en relación a una muestra de países de todo el mundo- la aplicación de las TIC en la administración y el liderazgo gubernamental.

Los objetivos del ranking son: (a) compartir buenas prácticas entre los países participantes, (b) mostrar la evolución del e-Gobierno en cada país, (c) identificar tendencias en el desarrollo del e-Gobierno, y (d) constituirse en una valiosa referencia para informes de investigadores y estudiosos.

La encuesta y ranking de e-Gobierno se sustenta en 9 indicadores principales y 32 subindicadores referidos al desarrollo del e-Gobierno y su contribución a las relaciones entre gobiernos y entre éstos y otros actores relevantes.

Los indicadores son: (1) Disposición e infraestructura para actuar en red, (2) Optimización de la eficiencia en la gestión, (3) Desempeño de servicios y aplicaciones en línea; (4) Portal Nacional, (5) Director de Información (CIO) estatal, (6) Promoción del e-Gobierno, (7) e-Participación e inclusión digital; (8) Gobierno Abierto; y (9) Seguridad Informática.

Los subindicadores correspondientes a los referidos indicadores son los siguientes:

(1) Disposición e infraestructura para actuar en red: 1.1 Usuarios de Internet, 1.2 suscriptores de banda ancha, 1.3 abonados a telefonía celular móvil

(2) Optimización de la eficiencia en la gestión: 2.1 Disposición optimizadora, 2.2 Integración de la arquitectura Institucional, 2.3 Sistemas administrativos y presupuestarios

(3) Desempeño de servicios y aplicaciones en línea: 3.1 e-Adquisiciones, 3.2 Sistemas de tributación, 3.3 Sistemas aduaneros, 3.4 Sisrema de e-Salud, 3.5 Servicio de ventanilla única

(4) Portal Nacional: 4.1 Navegación, 4.2 Interactividad, 4.3 Interfaz con el usuario, 4.4 Aspectos técnicos

(5) Director de Información (CIO) estatal: 5.1 Presencia del CIO, 5.2 Mandato del CIO, 5.3 Organizaciones del CIO, 5.4 Programas de desarrollo del CIO

(6) Promoción del e-Gobierno: 6.1 Mecanismo legal, 6.2 Mecanismo de habilitación, 6.3 Mecanismo de Apoyo, 6.4 Mecanismo de evaluación

(7) e-Participación e inclusión digital: 7.1 Mecanismos de e-Información, 7.2 Consulta, 7.3 Toma de Decisiones

(8) Gobierno Abierto: 8.1 Marco legal, 8.2 Sociedad, 8.3 Organización

(9) Seguridad Informática: 9.1 Marco legal, 9.2 Medidas contra el delito informático

2. Nueva Zelanda: ¿Cómo podría mejorar su posición en el ranking Internacional de e-Gobierno Waseda-IAC?

Fuente: “New Zealand is 13th (a notch lower) in Global e-Government Ranking”, 3/08/2015.

<http://www.unpan.org/Library/MajorPublications/UNEGovernmentSurvey/PublicEGovernanceSurveyintheNews/tabid/651/mctl/ArticleView/ModuleId/1555/articleId/46902/Default.aspx>

Fuente: CIO, New Zealand: <http://www.cio.co.nz/article/579379/new-zealand-13th-notch-lower-global-e-government-ranking/>

En el ranking internacional 2015 de e-Gobierno del Instituto de e-Gobierno de la Universidad de Waseda y la Academia Internacional de CIOs (IAC), Nueva Zelanda fue ubicada en la posición 13^º (ver tabla de posiciones en nota 1). A través de las 11 ediciones consecutivas del ranking, dicho país estuvo siempre en las primeras 15 posiciones, sin haber logrado –en ninguna oportunidad- ubicarse entre las primeras 10 posiciones.

Los expertos de Nueva Zelanda preguntaron al equipo a cargo de la encuesta y el ranking internacional de e-Gobierno de Waseda-IAC cómo podría dicho país llegar a ubicarse entre las 10 primeras posiciones. Las respuestas de los integrantes del equipo enfatizaron en los siguientes factores:

- (a) Infraestructura TIC:** este factor es clave, dado que potencia la administración y gestión gubernamental y ofrece a todas las personas la oportunidad de participar en la sociedad del conocimiento. El equipo señala que todos los países ubicados en las 10 primeras posiciones cuentan con una muy buena infraestructura para el desarrollo del e-Gobierno, además de exhibir aumentos en el número de usuarios de Internet y de suscriptores de banda ancha. También focalizan en la ampliación de la capacidad de banda ancha y en la construcción de infraestructura para la tecnología de nube. Señala el equipo que la importancia de la infraestructura para el desarrollo del e-Gobierno ya no se limita a ofrecer servicios para los usuarios de Internet, suscriptores móviles o conexiones de banda ancha, sino que además está estrechamente relacionada con el desarrollo de la integración entre los gobiernos locales y los nacionales. El equipo reconoce que la base para el desarrollo del e-Gobierno en un país depende de su sistema de Red Troncal del Gobierno y de su capacidad para conectar conjuntamente a todas las oficinas y departamentos de los distintos niveles territoriales.
- (b) Disposición para operar en red:** es otra área clave relacionada con la efectiva penetración de Internet en los países. Todos los 10 primeros países en el ranking han integrado las tecnologías Web 2.0 dentro de sus servicios electrónicos, habiendo logrado medir y mejorar el rendimiento con un alto nivel de “integración de los servicios”.
- (c) Interoperabilidad:** el intercambio de datos entre los organismos gubernamentales y entre los gobiernos locales y el gobierno central- es fundamental para lograr los avances deseados.

REFERENCIAS

Boletín e-Gobierno OEA/Red GEALC N° 79, noviembre 2012: “e-Gobierno y Gestión de Identidades”.

<http://portal.oas.org/LinkClick.aspx?fileticket=Sbjy8TLpzCE%3D&tabid=1729>

Número del Boletín e-Gobierno OEA/Red GEALC referido a la gestión de identidades en servicios de e-Gobierno. Tiene el propósito de contribuir a promover el aprovechamiento del potencial de las herramientas de gestión de identidades en los países de América Latina y el Caribe, en beneficio de los ciudadanos. Incluye relevantes testimonios, así como documentos y notas pertinentes. Los testimonios corresponden a los siguientes funcionarios y expertos entrevistados: (a) Steven Griner, Coordinador del Programa de Universalización de la Identidad Civil en las Américas (PUICA), OEA; (b) 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, Argentina; (c) César López, Especialista en gestión de identidad y biometría; ex CIO del Registro Nacional de Identidad y Estado Civil (RENIEC), Perú; (d) Santiago Paz, Director y fundador del Centro Nacional de Respuesta a Incidentes de Seguridad Informática de Uruguay (CERTuy)

España. INTECO/INCIBE: Guía sobre riesgos y buenas prácticas en autenticación online

<https://www.incibe.es/file/dQ2LIGywAc1c6KV20P101Q>

El reconocimiento y la confirmación de la identidad de los usuarios es una tarea primordial para garantizar que tanto los recursos como los servicios sean utilizados por los legítimos usuarios, ya sea los propios interesados o sus representantes legales.

El Instituto Nacional de Tecnologías de la Comunicación (INTECO) (que el 28/10/2014 se convirtió en INCIBE - Instituto Nacional de Ciberseguridad) publicó una nueva guía sobre riesgos y buenas prácticas en autenticación online, con los siguientes objetivos: (a) informar sobre las ventajas de la comprobación y verificación de la identidad de los usuarios en sus trámites vía internet (certificados, DNIE, firma electrónica, etc), (b) identificar los posibles riesgos para la seguridad y la privacidad, (c) ofrecer una serie de pautas y recomendaciones para prevenir y mitigar tales riesgos, y (d) aportar información útil para implantar mecanismos de identificación y verificación de identidad en Internet.

En dicha guía se exponen las características y los aspectos a tener en cuenta respecto en los procesos de identificación y verificación, sus diferentes tipos en función de diversos aspectos y las implicaciones legales a considerar. Asimismo se enuncian los principales riesgos y amenazas y una serie de buenas prácticas y recomendaciones para usuarios y desarrolladores.

Gamby, Randall: ¿Ha madurado por fin la autenticación basada en riesgo?

<http://searchdatacenter.techtarget.com/es/respuesta/Ha-madurado-por-fin-la-autenticacion-basada-en-riesgo>

Las tendencias vigentes en TIC (la nube, la movilidad, las redes sociales y los datos compartidos en línea), con cada vez más usuarios, aplicaciones, información y puntos de entrada, imponen crecientes necesidades de autenticación fiable en función del contexto.

La autenticación basada en riesgos consiste en determinar los debidos controles para identificar con precisión a un usuario basándose en una amplia gama de criterios y factores, tales como la ubicación geográfica, la dirección IP, la configuración y los servicios del sistema en uso (por ejemplo, el software antivirus). Por ejemplo, cuando un usuario solicita acceder a su cuenta desde una ubicación remota no utilizada previamente o usa un sistema que nunca antes había utilizado, el sistema lo detecta y le exige –además de ingresar su información de autenticación- responder una pregunta de validación o proporcionar información adicional, como su código postal.

La autenticación basada en riesgos ha evolucionado hacia un equilibrio adecuado entre seguridad, experiencia del usuario y coste.

Argentina. Jefatura de Gabinete de Ministros (2011): **Biometrías 2: Herramientas para la Identidad y la Seguridad Pública**, Buenos Aires

Acceso al texto completo: <http://www.biometria.gov.ar/media/74948/biometrias2.pdf>

Libro que reúne las experiencias de algunos de los asistentes al VI Congreso Internacional de Biometría de la República Argentina (CIBRA) desarrollado en la Ciudad Autónoma de Buenos Aires los días 14, 15 y 16 de Noviembre de 2011. Su mayor interés radica en la difusión de diversos conocimientos de aplicación biométrica desarrollados a través de experiencias en el ámbito de la Administración Pública Nacional e Internacional y del sector privado.

Su objetivo es difundir, entre el público interesado, algunas orientaciones e información específica. Por eso es que el orden de los artículos va desde las cuestiones generales hacia las más especializadas, que son abordadas desde los más diversos ángulos.

A través de sus capítulos se tratan las distintas categorías de métodos de autenticación habitualmente clasificadas de acuerdo al elemento utilizado: (a) factor de conocimiento: algo que el usuario conoce (por ejemplo, una contraseña, una frase o un número de identificación personal), (b) factor de posesión: algo que el usuario posee (por ejemplo, una tarjeta inteligente (smartcard), un dispositivo usb tipo token, una tarjeta de coordenadas, firma digital), y (c) factor de inherencia: rasgos conductuales o físicos que permiten identificar unívocamente a la persona través de patrones biométricos (ejemplo, verificación de voz, del rostro, de escritura, de huellas dactilares, de patrones oculares, secuencia de ADN). En caso de transacciones sensibles –con riesgo significativo- es usual combinar distintas categorías.

Wing, Bradford (2011): Normas y Biometría//En Argentina. Jefatura de Gabinete de Ministros (2011): **Biometrías 2: Herramientas para la Identidad y la Seguridad Pública**, Buenos Aires, pp. 51-70

<http://www.biometria.gov.ar/media/74948/biometrias2.pdf>

La razón básica para usar un sistema biométrico es descubrir la identidad o verificar la identidad declarada de una persona. Un sistema biométrico está diseñado para responder las siguientes preguntas: (a) ¿Es la persona la que dice ser?, (b) ¿La persona no es quien dice no ser?, (c) ¿Puede ser identificada una persona a partir de la información almacenada en el sistema?

El artículo se refiere primordialmente a los estándares nacionales e internacionales de autenticación biométrica, con claras descripciones de características, fortalezas y desafíos. Señala que los estándares sólo tienen sentido si son usados, y que sólo serán usados si: (a) sirven para el propósito con que fueron acordados, y (b) cubren las necesidades de los usuarios y de las instituciones prestadoras de servicios.

Si bien la concertación de estándares es un proceso continuo, las normas deben permanecer relativamente estables para poder ser usadas durante un período razonable de tiempo. Resalta la importancia de que los propietarios y usuarios de sistemas biométricos, así como la industria, el gobierno y la academia, se acerquen a los organismos de estandarización y participen en los procesos de desarrollo. Por su parte, los organismos de estandarización deben promover una adecuada representación de todos los grupos afectados por los estándares en proceso, así como garantizar que las normas en desarrollo estén basadas en el mejor conocimiento disponible y reflejen fielmente las necesidades de la comunidad.

García, L. Enrique (2014): Prólogo de la serie “Estado, Gestión Pública y Desarrollo en América Latina”, Buenos Aires: CAF.

Consultado en: <http://scioteca.caf.com/handle/123456789/795>

El prólogo del Presidente Ejecutivo de CAF -L. Enrique García- sobre la serie “Estado, Gestión Pública y Desarrollo en América Latina” señala que la comprensión y debate de los problemas del desarrollo latinoamericano enfrenta tres obstáculos con relevancia estratégica:

- (a) La búsqueda de conocimiento corre el riesgo de carecer de suficiente contextualización histórica y de no aprovechar el patrimonio conceptual disponible sobre el papel de los factores político-institucionales.
- (b) El debate resulta frecuentemente apropiado por una disciplina o enfoque que, en la búsqueda de simplificación y de parsimonia explicativa, desestima la presencia de variables imprescindibles para contemplar los procesos históricos, comprender la lógica de los desafíos y diseñar e implementar las estrategias necesarias para alcanzar y sostener el desarrollo en la región.

(c) Las barreras idiomáticas y regionales aún dificultan el aprovechamiento de novedades y de análisis relevantes para comprender la economía política de los procesos de desarrollo.

A través de la publicación de la serie el CAF procura contribuir a superar dichos obstáculos y a expandir la oferta de distintas modalidades de capacitación orientadas a las gerencias públicas de los países de la región. Su objetivo general es promover una cultura de excelencia en la gestión pública y compartir experiencias de diseño y ejecución de políticas públicas asociadas al fortalecimiento institucional.

Levi, M., Weber, M., Skocpol, T., Evans, P., Oszlak, O., Peters, B. G., ... Khademian, A. (2015). **El valor estratégico de la gestión pública. Trece textos para comprenderla.** Serie “Estado, Gestión Pública y Desarrollo en América Latina” Buenos Aires: CAF.

Consultado en: <http://scioteca.caf.com/handle/123456789/795>

[http://scioteca.caf.com/bitstream/handle/123456789/795/Tapa%2bLibro 2 CAF 2015 Versi on%20digital.pdf?sequence=1&isAllowed=y](http://scioteca.caf.com/bitstream/handle/123456789/795/Tapa%2bLibro%20CAF%202015%20Versi%20digital.pdf?sequence=1&isAllowed=y)

Resumen extraído de la Introducción

Compilación de artículos que tiene como propósito explorar posibles respuestas referidas a la relación entre el gobierno de lo público, las características del Estado, la administración pública, la gestión de lo público y las políticas públicas, y a cómo se diferencian y se articulan esas piezas de la vida social. Se trata de artículos ya publicados (en algunos casos hace 30 años) que aportan valiosos elementos de juicio para encarar desafíos centrales para poder forjar mejores políticas públicas en América Latina, y cuyo sentido y lógica es lo que se persigue comprender por medio de los textos seleccionados.

Por ejemplo, Peter Evans (1996) señala que la diferencia entre Estados predatorios y Estados desarrollistas consiste en que los primeros se apropian de la renta para su propio beneficio y los segundos la invierten en bienes públicos y en beneficio del desarrollo. El mecanismo que habilita la apropiación egoísta de los recursos estatales es una estructura administrativa de tipo patrimonialista formada por amigos, familiares y partidarios del gobierno que no distinguen la propiedad estatal de su propiedad privada y cuyo poder emana de los gobernantes. Por su parte, Merilee Grindle (2012) cuestiona el sentido común instalado que sugiere que un servicio público autónomo, profesional y experto sea sinónimo de buen gobierno. Paradójicamente, la discrecionalidad para atraer a las personas más calificadas para cada función es la que justamente permite una mayor flexibilidad para escapar a las rígidas leyes del servicio civil y al peso de una burocracia «arraigada».

O'Donnell, G., Cárdenas, M., Mann, M., Ziblatt, D., Oszlak, O., Geddes, B., ... Rockman, B. A. (2015). **Capacidades estatales. Diez textos fundamentales.** Serie "Estado, Gestión Pública y Desarrollo en América Latina". Buenos Aires: CAF.

Consultado en: <http://scioteca.caf.com/handle/123456789/715>

http://scioteca.caf.com/bitstream/handle/123456789/715/Libro_1_CAF_Capacidades_version%20WEB-RGB%20%28protect%29.pdf?sequence=1&isAllowed=y

En el intercambio académico y político solemos hallar diagnósticos que enfáticamente dictaminan que una gran parte de los problemas públicos y de desarrollo en América Latina son consecuencia de falta de "capacidad estatal". Sin embargo, ¿A qué nos referimos cuando hablamos de capacidad estatal?, ¿Qué implicancias tienen las diversas concepciones para definir prioridades y estrategias de desarrollo, y sobre su calidad y eficacia?

Dada la diversidad de perspectivas acerca de la noción de "capacidad estatal", los intercambios se tornan dispersos y confusos. En la actualidad, definir y medir la noción de capacidad estatal acarrea dos problemas. El primero se vincula con el hecho de que es multidimensional, que no existe consenso acerca de las dimensiones que la componen y que las diversas dimensiones que suelen incluirse se explican por diferentes factores. El segundo problema es que, más allá de su definición, ésta no puede dissociarse de la pregunta sobre capacidades para qué. No se requiere de las mismas capacidades para intervenir en distintos tipos de problemas públicos (por ejemplo, económicos, militares, de coordinación entre agencias). Por tanto, resulta primordial ajustar la definición de capacidad estatal al contexto sectorial en el que se precise intervenir, haciéndose particular referencia a los denominados «Estados fallidos» caracterizados por la pérdida del monopolio de la coacción en zonas geográficas que quedan bajo el poder de otros actores sociales: secesionistas, insurgentes, narcotraficantes, etc.

Los trabajos compilados en el volumen resumen las distintas perspectivas del vasto debate en torno a la "capacidad estatal", su forja e implicancias para los procesos políticos y de desarrollo socioeconómico.

Sanguinetti, P., Brassiolo, P., Ortega, D., Álvarez, F., Quintero, L., Berniell, L., ... Maris, L. (2015). **RED 2015: Un Estado más efectivo. Capacidades para el diseño, la implementación y el aprendizaje de políticas públicas.** Bogotá: CAF.

Consultado en: <http://scioteca.caf.com/handle/123456789/755>

El debate sobre las políticas públicas para el desarrollo se ha concentrado en definir las mejores intervenciones para promover el crecimiento y la inclusión, prestando menor atención a las capacidades de las agencias e instituciones gubernamentales concretarlas. Sin embargo, la evidencia está plagada de esfuerzos que no logran los impactos esperados por limitaciones en las capacidades de las agencias encargadas del diseño o la implementación de las intervenciones.

A través de esta edición del Reporte de Economía y Desarrollo (RED), CAF procura realizar un aporte al estudio y la comprensión de las capacidades del Estado para el diseño, la implementación y el aprendizaje de políticas y, de esta forma, contribuir a generar un debate constructivo que pueda favorecer el fortalecimiento de estas capacidades.

Los principales hallazgos del reporte giran en torno a los siguientes aspectos: (a) La calidad de la burocracia depende de las características de los funcionarios públicos y de las normas y procedimientos que guían, incentivan o limitan su accionar, (b) Contar con esquemas de compensación que permitan atraer a los mejores empleados y promover el esfuerzo es un primer requisito para mejorar la calidad de la administración pública, (c) la adecuada ejecución de las iniciativas de política requiere contar con un sistema de compras públicas capaz de proveer los suministros necesarios en cantidad y calidad suficientes en el momento oportuno, (d) la participación ciudadana puede ser un factor importante de control externo que promueva un mejor desempeño del Estado, (e) las TIC son herramientas con gran potencial para incrementar el poder que la ciudadanía tiene para mejorar el diseño e implementación de políticas públicas, al reducir los costos de coordinación entre ciudadanos para la acción colectiva y de interacción con las burocracias, y por ser además una vía de rápida y amplia difusión de información sobre el desempeño del Estado, (f) las constantes decisiones que se toman en el marco de la gestión de los recursos públicos presentan oportunidades para generar y sistematizar un conocimiento valioso para quienes diseñan e implementan programas públicos, (g) es necesario aumentar los beneficios esperados y reducir los costos de evaluar para los agentes encargados de tomar estas decisiones, y (h) para que el conocimiento generado con la evaluación se aplique en la gestión, es necesario promover una institucionalidad que favorezca la toma de decisiones sobre la base de la mejor evidencia disponible.