Modelo de Integración de Estándares para la Gestión de Identidad y Privacidad

Mag. Abogada. María del Carmen Becerra[1] , Programador Universitario Pedro Zarate[2], Mag. Lic. María Claudia Gomez[3]
[1,2] Instituto de Informática – Laboratorio de Análisis Forense e Informática Jurídica. Departamento de Informática – FCEFN-UNSJ
[3] Departamento de Informática - Directora del Proyecto de Investigación "Representación genérica de modelos conceptuales en el campo de los Sistemas de Información" FCEFN-UNSJ
mcbecerra2008@gmail.com,
pzarate@iinfo.unsj.edu.ar, cacugomez@yahoo.com.ar

Abstract. Este trabajo presenta un modelo para facilitar la gestión de la seguridad en el manejo de la identidad y privacidad. Se muestra la importancia y urgencia de este tema dado que ello es necesario y presta grandes beneficios para mejorar los servicios públicos. Se debe contar con estrictas medidas de seguridad basadas en la integración de normas, estándares y leyes más relevantes relacionadas con este tema, para mantener a salvo los datos personales. Se identifican el conjunto de prácticas y recursos de gestión, resultantes de la integración de estándares, y se discuten brevemente diversos aspectos involucrados en la formulación del modelo. El modelo propuesto permite establecer los pasos para que cualquier tipo de organización pública o privada, pueda realizar un manejo seguro de los datos sensibles de las personas.

Keywords: Identidad – Identidad Digital-Manejo de Identidad. Comparación de estándares. Modelo de Seguridad

1 Introducción

Con este trabajo se pretende brindar un modelo para que las organizaciones tanto públicas como privadas puedan gestionar la seguridad de la privacidad de los datos sensibles, con el fin de fortalecer la protección de datos conforme los estándares vigentes.

Se propone, caracterizar a la identidad digital como un derecho personalísimo y establecer su dimensión en una cuarta generación donde, la universalización del acceso a la tecnología, la libertad de expresión en la Red y la libre distribución de la información, juegue un papel fundamental [1], [2].

Estos derechos personalísimos, a la imagen, a la intimidad, al honor, a la reputación, a preservar la vida privada, así como cualquier otro del que resulte una emanación de la dignidad humana, están en los pactos internacionales y en nuestra Constitución. El ordenamiento positivo de nuestro país los ha tutelado, en diversas leyes como la Nº 11.723, Nº 24.766, Nº 25.326, Nº 25.506, Nº 26.388 que reformó el Código Penal, y cobran especial relevancia después de la entrada en vigencia del nuevo Código Civil y Comercial, que recoge la doctrina y la jurisprudencia imperante[3].

Las tecnologías biométricas han sido puestas en uso sin las medidas adecuadas de seguridad para la información personal que es resguardada. Las organizaciones han incorporado en su estructuras organizacionales, tanto el registro de asistencia biométrico (huellas dactilares, registro facial), como los teléfonos corporativos con características biométricas (voz, patrón de la retina). Los riesgos se han incrementado y sofisticado y hay una demanda de mayor eficacia, que requiere respuestas de la tecnología [4].

Se plantea un modelo de integración, donde las normas y estándares a ser evaluados, respondan a un modelo general de valuación de los sistemas de información, como conjunto de elementos interrelacionados para lograr un objetivo especifico.

La selección de estándares y normas se ha llevado a cabo utilizando el método de estudio de comparación de los mismos, se han creado plantillas para la comparación de las similitudes respecto a la gestión de la identidad y la privacidad.

El modelo propuesto, es una primera aproximación generada desde el proyecto referenciado, y está en proceso de contrastación.

2 Identidad Legal

La identidad se puede definir como conjunto de atributos y características que permiten individualizar a la persona en sociedad, pertenecientes a un individuo determinado, o compartidas por todos los miembros de una determinada categoría o grupo social. Según Rummens, el término proviene de la palabra francesa “identité” que tiene sus raíces lingüísticas en el sustantivo latino “identitas”, una derivación de “ídem”, que significa “lo mismo” [5].

El Estado, debe garantizar el derecho a la identidad, poseer una identidad es un derecho humano de cualquier ciudadano y, al mismo tiempo, es parte de las obligaciones que un Estado tiene para con sus ciudadanos, en este sentido el acta de nacimiento es tanto el primer reconocimiento de la existencia de un individuo, como el primer instrumento legal con que cuenta una persona para demostrar su identidad.

En Argentina, la Ley 17.671 es la que establece la identificación, registro y clasificación del potencial humano nacional, ella establece que la identidad- incluye el nombre, el apellido, la fecha de nacimiento, el sexo y la nacionalidad del individuo. Además es la primera prueba de existencia de una persona como miembro de una sociedad, como parte de una nación, y es aquello que lo caracteriza y lo diferencia de los demás ciudadanos. Actualmente, el Decreto Nº1766 del 2011, estableció un Sistema Federal de Identificación Biométrica, y tanto el D.N.I. como el pasaporte incorporan datos biométricos de las personas. La identidad la constituyen datos personales como el nombre, lugar de nacimiento, datos de filiación, nacionalidad, sexo, domicilio, fotografías, teléfono, correo electrónico.

La integran componentes físicos como: la huellas dactilares y plantares, el patrón del iris, el patrón de la retina, la forma de la mano, el patrón de las venas del dorso de la mano, la geometría de la mano, el rostro (registro facial), el reconocimiento vascular, las pulsaciones cardíacas, la identificación de la ondas cerebrales, ADN.

Los componentes de comportamiento como firma manuscrita, el análisis de los gestos, la forma de caminar, de gesticular. La voz se considera una mezcla entre componentes físicos y componentes de comportamiento. Existen elementos de identificación electrónica como el DNI, pasaporte, números de licencia y de seguridad social; números de tarjeta de crédito y de cuentas bancarias; nombres de usuario y contraseñas; incluyendo información financiera o médica, que contienen casi la totalidad de los datos que permiten identificar a una persona. Según la pertinencia corresponden a distintas áreas de las organizaciones, como muestra la Tabla 1.

Usos de datos personales / Aplicación en las Distintas áreas		Forense	Legal	Gubernamental	Financiero	Salud	Inmigración
De cara al Ciudadano	ID Criminal	X	X	X			
	Verificación/Identidad	X			X		X
	Vigilancia						X
	Voto			X			
	Salud			X			
De Cara al empleado	Pc móvil	X	X	X	X	X	X
	Acceso físico	X					
	Acceso remoto	X					
	Sistemas	X					
	Redes	X					
	Peritaje	X					
De Cara al cliente y/o usuario	E-Commercio	X	X		X		
	Transacción			X	X		
	Punto de venta						
	Auditoria			X			

Tabla 1. Ejemplo de esquema de uso de datos personales por areas dentro de las organizaciones

3 Manejo de la Identidad Digital

Las tecnologías de la información han generado un nuevo concepto de identidad: la digital. El perfil de la "persona virtual" se define en la red y se nutre de los contenidos que la misma proporciona respecto de un determinado individuo o compañía: la web otorga contenido, identifica e individualiza a la persona de una u otra manera.

Así, la identidad digital, representa las mismas características y actividades, que la identidad real, pero llevadas a cabo en internet, como consecuencia del crecimiento de las comunicaciones digitales. Esta identidad es a la que generalmente se refiere como "vida virtual".

Otros autores la conceptualizan, como "El conjunto de rasgos y características particulares, que una persona expresa a través de internet, forma una parte inescindible de la identidad personal de cada sujeto, en su faz dinámica, y más precisamente en su aspecto psicológico, social y moral".

La identidad digital se construye conforme lo enfatizan otros autores [6] de forma activa, aportando textos, imágenes y vídeos a Internet, participando, en definitiva, del mundo web. En los sitios de redes sociales, se construye a partir de un perfil de usuario, que a menudo se enlaza a perfiles de otros usuarios o contactos. En la identidad digital convergen muchos aspectos de carácter sociológico, cultural e incluso psicológico [7].

Para Benantar [8], es una representación de una entidad activa en la computadora. Dicha entidad puede ser física (usuario, servidor u otro dispositivo) o software. La identidad esta asignada a un identificador el cual a su vez contiene atributos y derechos los cuales están referenciados a un perfil, un sistema de manejo de identidades pretende que la creación, asignación de derechos o negación de permisos de un perfil sea lo más sencillo posible. Por lo tanto se puede definir el manejo de la identidad como la administración de la misma, bajo estándares establecidos para que la seguridad de la información sea la correcta.

4 Comparación de Normas y Estándares para la Gestión de Seguridad de la identidad.

Se partió de, realizar una búsqueda en los documentos publicados hasta el momento vemos que el proceso de autenticación de identificación biométrica se basa en las normas ISO/IEC 17.799, 27.001 y 27.002 (estándares centrados en la seguridad de la Información, COBIT (estándares centrados en la gestión), ITIL Estándares centrados en los organismos públicos, y ANSI NIST-ITL 378 estándares centrados en la seguridad de datos biométricos.

Para la correcta administración de la seguridad de la información, se deben establecer y mantener acciones que busquen cumplir con los tres requerimientos de mayor importancia para la información, estos son:

• Confidencialidad: Busca prevenir el acceso no autorizado ya sea en forma intencional o no intencional a la información. La pérdida de la confidencialidad puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la organización.

• Integridad: Busca asegurar que no se realicen modificaciones por personas no autorizadas a los datos o procesos, o que no se realicen modificaciones no autorizadas por personal autorizado a los datos o procesos, o que los datos sean consistentes tanto interna como externamente.

• Disponibilidad: Busca asegurar acceso confiable y oportuno a los datos o recursos para el personal apropiado. Diferentes organizaciones internacionales han definido estándares y normas que apoyan en diferente medida el cumplimiento de los requerimientos indicados anteriormente.

A continuación se detallan los estándares de mayor utilización a nivel mundial, y que fueron tomados como base para el modelo propuesto IRAM ISO/IEC 17.799. Esta norma internacional ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la

seguridad de una organización. En el punto 5.2 establece que la información tiene distintos grados de sensibilidad y criticidad. En el punto 9.23 administración de contraseñas de usuarios.

Las Normas IRAM ISO/IEC 27.001 y 27.002. Definen y documentan, los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización. Garantizan la protección y privacidad de los datos según lo requieran las legislaciones y si fueran aplicables, las clausulas relevantes contractuales.

Existen además, normas como la ISO 24.760 e ISO 29.100, que proporcionan un marco de referencia de alto nivel para la protección de los datos personales, y regulan la Gestión de identidad y Privacidad. Aportan a la gestión de privacidad las ISO 29134, e ISO 29151, ISO 29190/91 que presentan un modelo de evaluación de la capacidad en privacidad.

COBIT Acrónimo de "Control Objectives for Information and related Technology" (Objetivos de Control para la Información y Tecnologías Relacionadas), es un estándar desarrollado por la Information Systems Audit and Control Foundation (ISACA), la cual fue fundada en 1969 en EE.UU., y que se preocupa de temas como gobernabilidad, control, aseguramiento y auditorias para TIC.

Actualmente tiene más de 60.000 miembros en alrededor de 100 países. Esta organización realiza eventos y 239 conferencias, y desarrolla estándares en TI de gobierno, aseguramiento y seguridad, siendo COBIT el más importante. El rol de COBIT 5 en la estrategia de seguridad, objetivos de control, nuevo marco para la gobernanza en TIC´S, y guías de COBIT 5 sobre seguridad y riesgo.

En los últimos 5 años ha cobrado fuerza debido a que fue desarrollado en específico para el ámbito de las TIC. ITIL Acrónimo de "Information Technology Infrastructure Library", ITIL es una norma de mejores prácticas para la administración de servicios de Tecnología de Información (TI), desarrollada a finales del año 1.980 por entidades públicas y privadas con el fin de considerar las mejores prácticas a nivel mundial. El organismo propietario de este marco de referencia de estándares es la Office of Government Commerce, una entidad independiente de la tesorería del gobierno británico. ITIL fue utilizado inicialmente como una guía para el gobierno de británico, pero es aplicable a cualquier tipo de organización.

Los Estándares ANSI/NIST-ITL son estándares que se aplican internacionalmente para proteger los datos biométricos. El propósito de esta norma es que un sistema biométrico dactilar pueda realizar procesos de verificación de identidad e identificación, empleando información biométrica proveniente de otros sistemas.

Normas y Estándares	ISO/IEC 17799	ISO/IEC 27001/02	ISACA-COBIT	ITIL	ANSI NIST/ITL (Ansi 378)
De cara al ciudadano	▪	▪	▪	▪	▪
De cara al empleado	▪	▪	▪	▪	
De cara al cliente y/o usuario	▪	▪	▪		

Tabla 2. Comparación de las características de los modelos de estándares.

El modelo se baso en la evaluación de normas y estándares, que proporcionan una base solida para el cumplimiento de los objetivos de la Organización, en cuanto a la seguridad de los datos personales. En la Tabla 2, se compararon los modelos y normas presentadas anteriormente y se contrastaron sus puntos fuertes y débiles en cuanto a gestión de seguridad de la información, estableciendo que "■" significa una fortaleza del modelo/norma relacionada con las características evaluadas, mientras que un espacio en blanco significa que hay una debilidad. Así por Ej. Los modelos que tienen más fortalezas en la relación a la gestión de capacidad de servicio de TI, son el modelo ITIL [9] y las Normas ISO/IEC 27.001 y 27.002 permiten que la información y la tecnología relacionada se rijan y se gestionen de manera integral en toda la empresa [10].

5 Modelo de Integración de Estándares para la Gestión de Identidad y Privacidad

Las Organizaciones desarrollan un conjunto de actividades y procesos, que deben gestionarse sistemáticamente de tal forma que permitan el cumplimiento de sus objetivos [11].

En el modelo general se evalúan las normas y estándares de seguridad, Figura 1; en primer lugar se detecto el estado del arte de las normas y estándares, luego se las comparó en función del uso e impacto de cara al ciudadano, de cara al empleado y de cara al usuario.

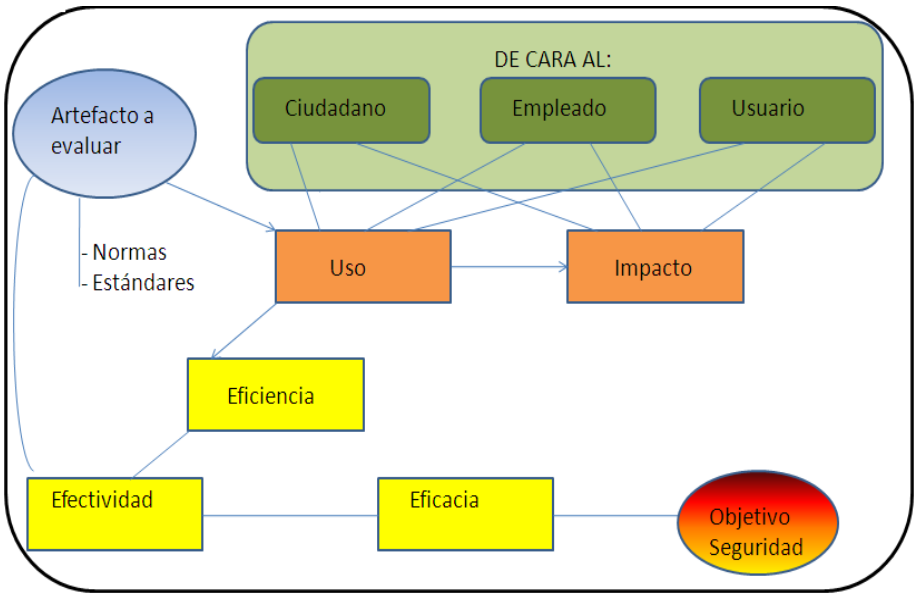

Fig. 1. Modelo General

Se midió el impacto desde estas tres perspectivas y la eficacia mediante el cumplimiento del principal objetivo que es la seguridad, este análisis se hará previo a su implementación, formulando criterios de evaluación que permitan ponderar su importancia en la protección de la privacidad [12].

La incorporación del Objetivo individual y organizacional y conceptos como el de efectividad que se basa en la eficacia (cumplimiento de Objetivos) y la Eficiencia (relación insumo/producto) pretende realizar una representación de Los sistemas de Información desde la perspectiva de su análisis cuantitativo y cualitativo.

De esta forma todos los artefactos TI, en la mayoría de los casos representados por proyectos de software[13], los que generalmente son evaluados mediante métricas específicas, requieren de una perspectiva desde las diferentes ciencias, lo que nos lleva a pensar que los SI necesitan de una visión interdisciplinaria[14].

6 Conclusiones

El aumento de la regulación y la legislación sobre la privacidad también esta impactando en los entornos TI. La adopción de modelos y normas facilita la rápida ejecución de los buenos procedimientos y ayuda a evitar retrasos innecesarios en el desarrollo de nuevos enfoques. Todas las empresas tienen que adaptar el uso de modelos y establecer normas para ajustar sus requisitos individuales.

Cada organización debe establecer su propia estructura de gestión y recoger en todos ellos las recomendaciones que resulten más útiles. El uso de estándares ayuda al cumplimiento de las leyes, reglamentos, acuerdos contractuales y políticos y a ganar en ventajas competitivas sobre otras organizaciones [15].

Finalmente es muy importante, como con este modelo general para la gestión de la seguridad va ha ser evaluado de cara al ciudadano, de cara al usuario y de cara al empleado, porque es fundamental medir la efectividad y la eficiencia, teniendo en cuenta la eficacia y como se usa e impacta sobre estas tres perspectivas. Pretende ser un aporte ante la preocupación internacional sobre la gestión de la identidad, tanto en el ámbito ciudadano como en el corporativo.

7 Referencias

[1] Ossorio, Manuel, "Diccionario de Ciencia Jurídicas, Políticas y Sociales", Heliasta, 2005, Pág. 240.

[2] http://www.oei.es/revistactsi/numero1/bustamante.htm#1a

[3] Bueres Alberto, Código Civil y Comercial de la Nación analizado, comparado y concordado. 1ra Ed. Bs.As. Ed. Ammurabi. ISBN 978-950-741-680-4

[4] Becerra. Navarro Mirta, Becerra, María del Carmen. Gestión Integral de Infraestructuras Criticas en las Organizaciones Locales alineados a las Normas IRAM ISSO 27.001 y 27002. WSI - II Workshop de seguridad informática CACIQ 2013

[5] Borghello Cristian, Temperini Marcelo G. JAIIO. Suplantación de Identidad Digital como delito informático en Argentina.

[6]La gestión de la identidad digital: Una nueva habilidad informacional y digital. BID. Universidad de Barcelona http://bid.ub.edu/24/giones2.htm

[7] http://blog.segu-info.com.ar/2012/07/como-se-construye-una-identidad-digital.

[8] Benantar, M.Access Control Systems-Security-Identity Management and trust Models New York:Springer.2006.

[9] Alleinni Féliz-Sánchez*, Jose Antonio Calvo-Manzano. Comparison of models and standards for implementing IT service capacity management. www.redalyc.org/pdf/430/43038629008.pdf

[10] El derecho informática y la gestión de seguridad de la información una perspectiva con base a la norma Iso 27001. Revista del Derecho 2008. Biblioteca de Ciencia y Técnica de la Nación

[11] Jacobson, I; Booch, G; Rumbaugh, J. El proceso unificado del desarrollo de software. Pearson 2000.

[12] Object Management Group, Inc. OMG. http://www.omg.org/2016.

[13] Gonzalo Perez-Tomé Estevez.Estudio sistemático de literatura de metodologías para la obtención de requisitos de privacidad.2015.www.dit.upm.es/…/TFM

[14]Diana M.Castillo Pinzon, DM. Enfoque para combinar e integrar la gestión de sistemas.2010.ISBN 978-958-8585-06-2

[15]Burgos Salazar, Jorge; Pedro G. Campos. Modelo para Seguridad de la Información en TIC. Web: ceur-ws.org/Vol-488/paper13.pdf