Implementation of Multi-Factor Strong Authentication Services and Confidentiality, for the Protection of Electronic Documentation

Felipe Andrés Corredor, M.Sc.[1], Leonel Álvarez Pabón, Est.[1], Diana Cristina Franco Mora, M.Sc.[1], and Andrés Felipe Ardila, Est.[1]

[1] Universidad de los Llanos, Colombia, felcorredor@unillanos.edu.co, lalvarez@unillanos.edu.co, dfranco@unillanos.edu.co, andres.ardila@unillanos.edu.co

***Abstract*– This research presents a review of context in the field of computer security about document management systems; in turn it generates an alternative process design and IT development, which permits the effective incorporation of multi-factor strong authentication services and confidentiality to a document management system, focused on security of electronic documentation. They worked with officials from the University of the Llanos, so that the requirements were accurate and then to test the system in a simulated scenario; with three modules load of documents and biometric fingerprint systems. For this, performance tests were applied, always focusing on security.**

***Keywords*— Security, Strong Authentication, multifactor authentication, electronic documentation, service confidentiality.**

Digital Object Identifier (DOI): http://dx.doi.org/10.18687/LACCEI2015.1.1.247
ISBN: 13 978-0-9822896-8-6
ISSN: 2414-6668

Implementación de los servicios de autenticación fuerte multifactor y confidencialidad, para la protección de documentación electrónica

Felipe Andrés Corredor, M.Sc[1], Leonel Álvarez Pabón, Est.[1], Diana Cristina Franco Mora, M.Sc. [1] y Andrés Felipe Ardila, Est.[1]
[1]Universidad de los Llanos, Villavicencio, Meta, Colombia, felcorredor@unillanos.edu.co, lalvarez@unillanos.edu.co, dfranco@unillanos.edu.co, andres.ardila@unillanos.edu.co

Resumen– Este investigación plantea una revisión de contexto en el campo de la seguridad informática sobre sistemas de gestión documental; a su vez genera una alternativa de proceso de diseño y desarrollo de TI, que permite incorporar eficazmente los servicios de autenticación fuerte multifactor y confidencialidad a un sistema de gestión documental, enfocado en la seguridad informática de documentación electrónica. Se trabajó con funcionarios de la Universidad de los Llanos, para que los requerimientos fueran precisos y posteriormente poder probar el sistema en un escenario simulado; con tres módulos de carga de documentos y sistemas biométricos de huella dactilar. Para ello se aplicaron pruebas de desempeño, siempre enfocándose en la seguridad informática.

Palabras Clave— Seguridad Informática, Autenticación Fuerte, autenticación multifactor, documentación electrónica, servicio de confidencialidad.

I. INTRODUCCIÓN

La sociedad genera información de manera exponencial y gran parte de esta se organiza en documentos, los cuales deben ser procesados con mecanismos tecnológicos que permitan la toma de decisiones corporativas. Aunque el desarrollo de sistemas de gestión documental no ha significado un obstáculo importante para el tratamiento ágil y oportuno de la información, la implantación contundente de estos sistemas a nivel organizacional y de seguridad de la información (**SI**), se ve afectada por las dudas que se generan en lo referente a la protección efectiva de los documentos electrónicos que allí reposan.

El contexto dispone de varios sistemas de gestión documental, algunos de licenciamiento libre (como Orfeo GPL y Alfresco), sin embargo no disponen de documentación de arquitectura de SI y la protección completa, debe darse con herramientas externas, lo que dificulta su adopción.

Es importante indicar que cuando se habla de SI, hay que ser muy cuidadoso para construirla, de tal manera que el costo del esfuerzo y otros recursos, sea razonablemente proporcional a lo que se quiere proteger [9]. En el caso de la protección documental, muchas organizaciones definen políticas de seguridad, confidencialidad y privacidad de información y usan diversos mecanismos tecnológicos de SI.

Los mecanismos aquí utilizados, por su gran potencial y bajo costo de implementación y ejecución son la autenticación y la biometría de huella dactilar, así como mecanismos criptográficos y derivados (criptografía simétrica, hash, TLS y firmas digitales) que garanticen la confidencialidad.

Para los procesos de autenticación se plantean tres elementos; lo que conoces, lo que tienes y lo que eres [10]; los cuales combinados estratégicamente (según el problema), posibilitan la autenticación Multifactor, mejorando los niveles de SI. Por un lado; el sólo uso de passwords ("lo que sabes") no es una medida de protección contundente y suficiente, (por las capacidades computacionales disponibles para realizar ataques de fuerza bruta a bajo costo) lo que conlleva al uso de otro factor, como la biometría ("lo que eres").

En el caso de la biometría; la investigación científica ha demostrado que algunas características físicas son lo suficientemente únicas y persistentes a lo largo de la vida; entre las cuales se tienen las huellas dactilares, el iris o los patrones de voz [11].

En esta investigación, partiendo de lo anterior, se generó un sistema de arquitectura *multitier*, con autenticación multifactor, capacidades criptográficas y de firmas digitales; convirtiéndose en una alternativa de solución verificada, para adoptar de manera adecuada los servicios de SI más relevantes en un sistema de gestión documental, en el cual se desarrollaron varios módulos que fueron implementados con tecnologías abiertas, apoyado de un protocolo propio, hardware de autenticación biométrico y librerías de seguridad de GNU/Linux, java y php.

II. CONTEXTUALIZACIÓN DEL PROBLEMA

Según la asociación colombiana de ingenieros de sistemas, a través de la V encuesta latinoamericana de seguridad de la información del año 2014; de 11 temas fundamentales para la seguridad, el de mayor relevancia para los encargados de la SI

es la Fuga de Información sensible con un 65,3% y en el que también se desataca la privacidad y protección de la información con un 55,4% [2]. El mismo estudio plantea que el 41% de las empresas latinoamericanas tiene poco entendimiento de la SI y esto es uno de los mayores obstáculos para implementar la SI en la organización.

Según Kroll, en la Encuesta global sobre fraude; En 2013-2014, el 22 % de las empresas fueron víctimas de fraude por Robo de información y es la segunda forma más común de fraude. Según este mismo estudio; en Colombia el 90 % de las empresas se siente expuesta a fraude y el 47% afirma que es debido a la rotación del personal. [4].

Las tendencias en ciberdelincuencia a nivel corporativo indican un incremento en delitos contra la privacidad (espionaje y robo entre otros…), los cuales le han costado a Colombia más de 870 mil millones de pesos, en un solo año y con un 64% de adultos que han sido víctimas de algún ciberdelito [3]. Los cuales se pueden mitigar con los servicios de confidencialidad y autenticación fuerte. Protegiendo los documentos desde la comunicación a través de canales cifrados, el almacenamiento con cifradores simétricos y complementando con un servicio de no repudio, a través de firmas digitales.

Las organizaciones son conscientes de los riesgos de SI a los que están expuestos sus documentos y por ello se plantea en [1], que 74% de las organizaciones a nivel global ha definido una política para la clasificación y el manejo de los datos sensibles como una medida de control para el riesgo de fuga de datos. También, aquí se plantea que el 72% de las organizaciones en el mundo, observan un aumento en el nivel de riesgo debido a mayores amenazas externas. Pero también se plantea por ACIS que el 41% de las empresas latinoamericanas tiene poco entendimiento de la SI [2] y esto es uno de los mayores obstáculos para implementar la SI.

En el contexto existen sistemas de gestión documental, como los relacionados en la tabla 1, pero no documentan una arquitectura de seguridad robusta. Y no se evidenciaron estudios orientadores de arquitecturas de seguridad para este tipo de sistemas.

TABLA I
SISTEMAS DE GESTIÓN DOCUMENTAL

	AUTOR	Portabilidad	Base de Datos	LICENCIA
orfeo	Jairo Losada, Denis López y otros	GNU/Linux, Windows, FreeBSD, Unix	PostgreSQL, Oracle y MS SQL Server	GNU/GPL
Alfresco	Alfresco Software Inc.	Multiplataforma	PostgreSQL, Oracle,SQL Server, MySQL, y DB2	Community Edition - GPL 2
nuxeo	Nuxeo SA	Linux, Mac OS X y Windows (Multiplataforma)	PostgreSQL, Oracle,SQL Server, MySQL, y DB2	LGPL
openKM	OPENKM	GNU/Linux, Windows, Mac OS, Unix	MySQL, PostgreSQL, Oracle o SQL Server.	GNU/GPL
aurea	Yerbabuena software	Multi-plataforma. Cualquier OS con soporte JAVA. Se recomienda GNU/Linux	PostgreSQL Server , Oracle 10 y 11 Mysql , Microsoft SQL Server.	Privativa

Lo cual deja la protección de documentos electrónicos, en manos de herramientas complementarias al sistema de gestión documental. Quedando entonces la implementación adicional de servicios de SI relacionados al tema de la protección de documentos o apoyarse de la computación en la nube (con los riesgos que esto acarrea sobre información sensible) y como ya se dijo anteriormente; a las organizaciones le es difícil y complejo la adopción de la SI.

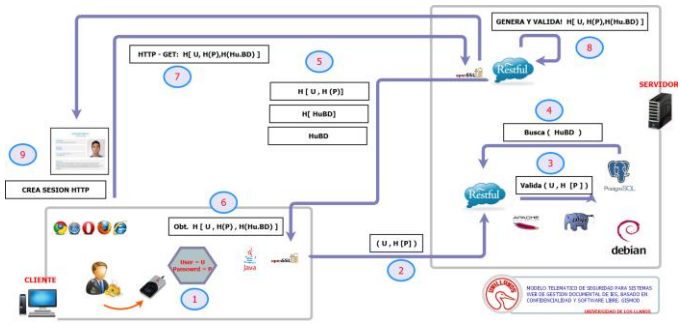
III. DISEÑO

Según el decreto de MINTIC 2609 de 2012, el Sistema de gestión documental debe incorporar dentro de sus características; conformidad, interoperabilidad, seguridad, meta descripción, disponibilidad y acceso, adición de contenidos, diseño y funcionamiento, gestión distribuida y neutralidad tecnológica [12], En lo referente a SI se recogieron los aspectos legales referentes a las leyes; 1273 de 2009[13], 1581 de 2012 (con el respectivo decreto 1377 de 2013) [14] y la ley 1712 de 2014 [15]. En resumen se acogen las disposiciones relacionadas con los riesgos que son delitos (acceso abusivo a un sistema informático. interceptación de datos informáticos. violación de datos personales, hurto por medios informáticos y semejantes), con la protección de información personal y finalmente con la transparencia de la información pública y la necesidad de clasificar los documentos.

En esta fase se contó con el apoyo adicional de la jefe de archivo de la Universidad de los Llanos y dos expertos en SI. Se determinó desarrollar una solución de autenticación fuerte multifactor de dos vías (*web y standalone*); apoyándose de la biometría de huella dactilar, como factor de identificación mas no de autenticación [9], quedando definida la arquitectura del módulo de autenticación como se observa en la Figura 1. Y las Notaciones usadas como se presenta en la tabla II.

TABLA II
NOTACIÓN USADA EN LA DEFINICIÓN DE LA ARQUITECTURA

Símbolo	Descripción
H:	*Resumen hash sha512*
U	*Texto plano del usuario*
P:	*Texto plano de la contraseña*
	Huella dactilar binaria capturada por el SDK
Hu:	*digitalPersona*
HuBD	*Huella dactilar serializada en la base de datos*
H[P]	*hash del texto plano de la contraseña*
HTTP-GET	*Petición HTTP-GET para generar sesión web*



Arquitectura del modelo de autenticación biométrico
Figura 1

La siguiente tabla (Ver Tabla III), presenta la descripción del proceso metodológico que sigue la autenticación, sobre la arquitectura diseñada:

TABLA III
METODOLOGIA DEL SISTEMA PARA AUTENTICACIÓN FUERTE

1	[C] El Usuario define la forma de autenticación, vía web o standalone (biométrica). El módulo cliente obtiene U y P.
2	[C] Se genera el Hash de P; H[P], se inicia un canal cifrado con OpenSSL y se transfiere U y H[P] al servidor web.
3	[S] El servidor valida la información de autenticación del usuario: U y H[P].
4	[S] El servidor busca la Huella correspondiente a ese usuario (HuBD) en la Base de datos. .
5	[S] EL servidor genera dos Hash; el de la Huella Obtenida de la Base de datos HuBD y el del usuario, combinado con el Hash del password recibido del cliente. Estos datos junto con HuDB son enviados a través de un canal cifrado al cliente.
6	[C] El cliente genera el Hash de los datos recibidos H[u, H[P], H(Hu, BD)].
7	[C] Con la llave de sesión generada, el cliente consume el Web Service de autenticación, enviando por el método GET de HTTP la llave de sesión.
8	[S] EL web Service valida, la llave de sesión.
9	[S] Si es correcta se permite el acceso al módulo funcional, si es incorrecto, aparece un mensaje de autenticación inválida.

El contexto ofrece esquemas de autenticación multifactor de varias fases; Algunos con enfoque específico para usuarios móviles, basados en criptografía simétrica y de dos factores, apoyado de *Smart cards* [6] y [8], también se plantea una autenticación basada en passwords y biométrica sobre la dinámica de los golpes de teclado [7],

El mecanismo de autenticación se diseño siguiendo el sigue el esquema de seguridad planteado por [5]; Fase de iniciación (Disposicion de servidores Web y Base de datos, así como el cliente con el driver del lector biométrico y el módulo de software ejecutándose), Fase de registro (el admin del sistema desde el modulo administrativo web, crea los usuarios necesarios), Fase de login (El usuario procede a determinar la vía del inicio de sesión) y Fase de autenticación (Se validan los factores de autenticación, se decide el ingreso y se controla el acceso).

Para la protección documental electrónica se definieron las siguientes operaciones restrictivas que a su vez estructuran cada nivel de protección requerido, son de obligatorio cumplimiento en cada nivel según relación y son automáticamente controlados por el sistema.

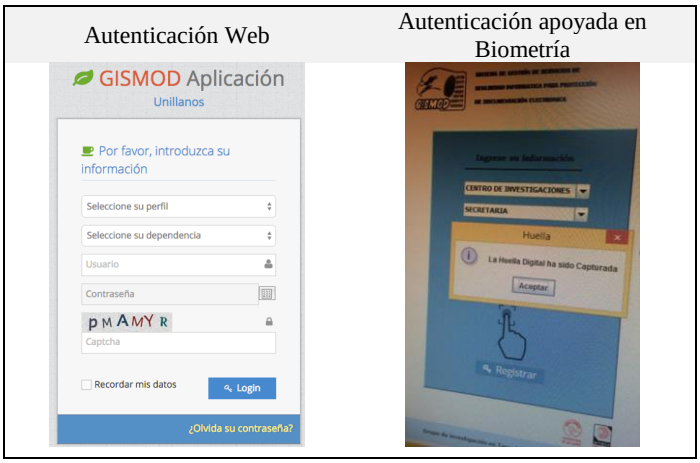
TABLA IV
RELACIÓN DE OPERACIONES OBLIGATORIAS PARA CADA NIVEL DE PROTECCIÓN

Operaciones restrictivas	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Cifrado simétrico bajo (AES 128 bits)		X		
Cifrado simétrico medio (AES 192 bits)			X	
Cifrado simétrico Alto (AES 256 bits)				X
Firma Digital sobre el documento.			X	X
Comprobación de Huella (verificar la huella dactilar desde el lector)				X
Transmisión por canal cifrado SSL		X	X	X
Configuración permisos obligatoria	X	X	X	X
Otorgar permisos individuales			X	X

IV. DESARROLLO

Para el desarrollo se dispuso un servidor en internet, con Debian GNU/Linux 7.6, motor de base de datos postgresql 9.1, Apache 2.2, php5, simple-captcha, Laravel 5, dompdf, tomcat7, highcharts y OpenSSL. El cliente se dispuso con Sistema Operativo Windows 7, Java JRE y JDK, API java Mail.

Se desarrolló la autenticación de dos vías y se desplego en el servidor del proyecto, para pruebas, quedando así:



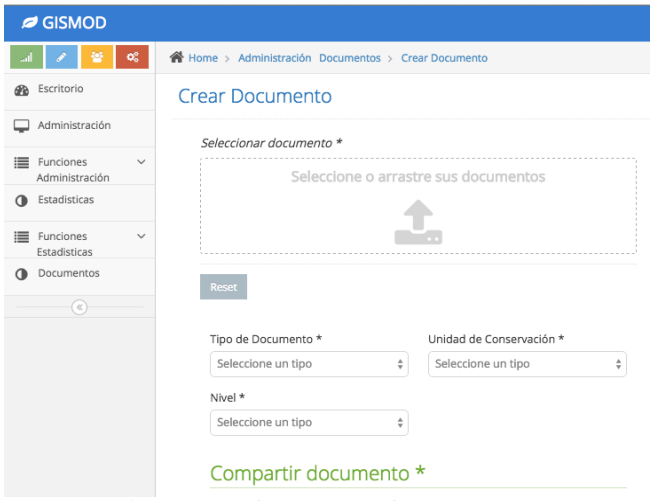
Interfaz del módulo de autenticación biométrico
Figura II

La autenticacion web (izquierda) desarrollada en php5, laravel 5 y html. La autenticacion biométrica (derecha) fue desarrollada en java, con la API del lector biométrico de digital persona.

La interfaz de gestión de información del usuario autenticado presenta la información personal, que puede editar, asi como una serie de alarmas y notificaciones en la esquina superior derecha, a través de la cual se le notifican todas las transacciones documentales con la que ha estado vinculado.

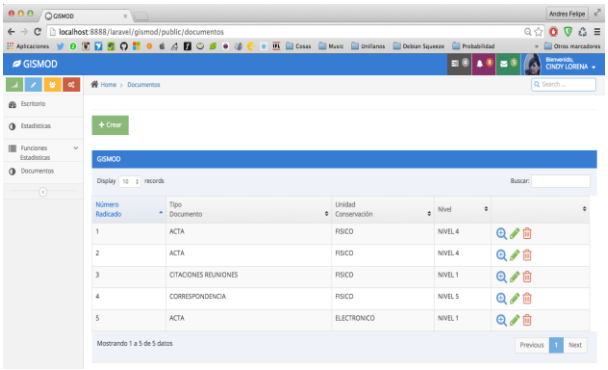
Interfaz del módulo de Usuario autenticado – Gestión de Información.
Figura III

Los servicios de confidencialidad y no repudio, se basaron en las librerías de php5; mcrypt y gnupg, que permiten implementar el cifrado simétrico y la firma digital respectivamente. El módulo de control de acceso valida las restricciones sobre cada documento según su nivel y permite al usuario realizar las operaciones respectivas sobre el documento. El usuario iniciará creando un documento, arrastrando sobre el panel y compartiéndolo, desde la interfaz web. Ver figura siguiente:



Interfaz web, del módulo de Creación de documento..
Figura IV

Finalmente una vez aplicadas las operaciones tanto de usuario, como las automáticas, se presenta el listado de documentos (Administrador de documentos),



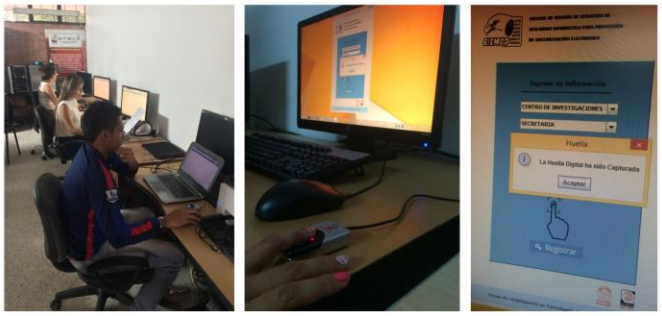
Repositorio de documentos electrónicos – Modulo administrador.
Figura V

IV. Análisis y discusión de resultados

Las características de un sistema con este enfoque están relacionadas con el planteamiento de [6], de las cuales, este sistema asume y cumple las siguientes: registro único, Prevención de fraude, El password es cambiado libremente por el usuario, Baja sobrecarga de la comunicación, Prevención de ataques internos, Establecimiento de llave de sesión. Además se le incorporó teclado aleatorio, captcha, biometría de huella dactilar, control de acceso, y clasificación de información…

Las pruebas se realizaron con tres funcionarios de la universidad de los Llanos (específicamente de la facultad de ciencias básicas e ingeniería) y el apoyo del grupo de investigación GITECX. Se ejecutaron transacciones reales, paralelas a las que se realizaban normalmente en producción. En la siguiente figura se presentan las actividades de la fase de

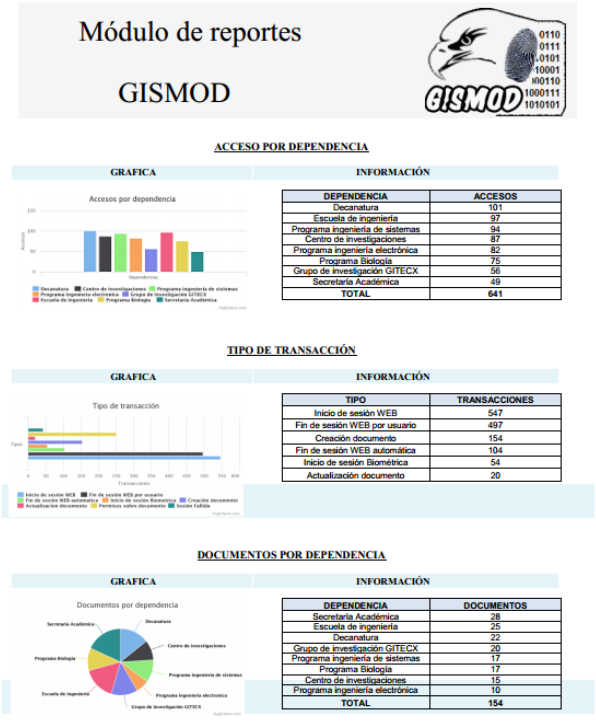
pruebas, donde se realiza inicio de sesión concurrente, en tres estaciones de trabajo, dispuestas con lectores biométricos, escáner e impresora de etiquetas.



Pruebas en Laboratorio de Tecnologías Abiertas, con Funcionarios.
Figura VI

Durante las pruebas no se afectaron la capacidad de concurrencia del servidor, ni se afectó significativamente el ancho de banda.

Se realizaron verificaciones sobre el módulo de reportes, que están relacionados con accesos al sistema, rendimiento, transacciones y documentos. Los reportes se envían automáticamente al email y son exportados por el sistema a PDF, cuando el usuario lo requiere. A continuación se presenta la primera página del reporte generado por el sistema.



Módulo de reportes generado automáticamente por el sistema
Figura VI1

Una vez terminado el desarrollo se organizó con 14 estudiantes de quinto semestre de ingeniería de sistemas; un taller orientado a la seguridad de accesos al sistema, rendimiento, transacciones y documentos los web services y su adecuada implementación, así se logró el apoyo de ellos a la realización de pruebas.

Taller de seguridad, realizado con estudiantes de Ingeniería de Sistemas
Figura VII1

V. Conclusiones

Colombia viene fortaleciendo su marco normativo que respalda la gestión de la documentación en las organizaciones. Pero las herramientas de gestión documental que dispone el contexto, son principalmente para otros países como Estados Unidos y Europeos), Orfeo es Colombiano y ha asumido aspectos legales nacionales para no presentar limitantes a los usuarios Colombianos, ya que los fabricantes en su mayoría no se interesan por tener en cuenta el marco legal.

Para el Sistema de gestión documental es fundamental disponer permanentemente de los módulos de autenticación y control de acceso (con su respectivo validador de restricciones), y un reporte rápido para la toma de decisiones, enviado automáticamente.

El uso de tecnologías libres es de amplia suficiencia y eficiencia para el desarrollo de sistemas de gestión documental y mecanismos de seguridad que permiten mitigar el riesgo de fuga o robo de información.

Agradecimientos

Los autores expresan su gratitud a Dios y sus Familias, quienes siempre apoyaron este proceso. De igual manera, al grupo de investigación GITECX y la Universidad de los Llanos por creer en este proyecto de investigación y financiarlo.

Referencias

[1] Ernst & Young , XIV Encuesta Global de Seguridad de la Información, http://www.ey.com/Publication/vwLUAssets/Salir_de_la_niebla_para_entrar_a_la_nube/$FILE/XIV_EGSI_Salir_niebla_%20para_entrar_nube.pdf

[2] Cano J. Saucedo G, et ál, V encuesta latinoamericana de seguridad de la información, http://acis.org.co/fileadmin/Base_de_Conocimiento/XIV_JornadaSeguridad/ELSI_2014.pdf
[3] Symantec, Reporte Norton 2013, http://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-colombia.es.pdf
[4] Kroll, 2013/2014 Informe Global sobre Fraude, http://fraud.kroll.com/wp-content/uploads/Reporte%20de%20Fraude%20Kroll%202013-2013%20Espanol%20-%20WEB.pdf
[5] Fan Wua, Lili Xu, ét al, A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks, Computers and Electrical Engineering.
[6] Daojing H, Maode M, A strong user authentication scheme with smart cards for wireless communications, Computer Communications.
[7] M. Karnana,∗, M. Akilab, Biometric personal authentication using keystroke dynamics: A review, Applied Soft Computing, Applied Soft Computing.
[8] Ding Wang, Ping Wang Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks, Ad Hoc Networks.
[9] The Basics of Information Security. DOI: http://dx.doi.org/10.1016/B978-0-12-800744-0.00002-6.
[10] Syngress, The Three Elements of Authentication, Chapter 13.
[11] Resistance Strategies: Authentication and Permissions, Chapter 7: Resistance Strategies: Authentication and Permissions.
[12] Ministerio de las TIC, Decreto 2609 de 2012. http://www.mintic.gov.co/portal/604/articles-3528_documento.pdf
[13] Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos", Ley 1273 de 2009, http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf
[14] Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html
[15] Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública, http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html

Authorization and disclaimer

Authors authorize LACCEI to publish the paper in the conference proceedings. Neither LACCEI nor the editors are responsible either for the content or for the implications of what is expressed in the paper.