UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Visión Electrónica
Más que un estado sólido
https://doi.org/10.14483/issn.2248-4728

VISIÓN ELECTRONICA
A Case-study Vision

SANI: Assistant for Information Security Auditing on ISO/IEC 27001

SANI: Asistente para Auditorías de seguridad de la información sobre ISO/IEC 27001

Diana Cristina Franco-Mora[1], *Hernán Oswaldo Porras-Castro*[2], *Felipe Andrés Corredor-Chavarro*[3], *Cristian Calderón-Bogotá*[4]

INFORMACIÓN DEL ARTICULO

Enviado: 30/11/2019
Recibido: 05/12/2019
Aceptado: 27/12/2019

ABSTRACT:

Information security is a fundamental aspect to any organization, not something exclusive to large companies. Implementing good practices in security management is relevant to being competitive in the context, however, adopting a standard in this regard is a tedious and expensive process for small companies. Audits are part of the proper management of information security, as these help to prevent incidents and mitigate risks on information assets. Many auditing applications are developed and executed in private technological settings, are expensive and not available to the community, or focus on functionality, but have serious difficulties in guaranteeing or documenting confidentiality and anonymity services. With this problem in mind, SANI, an alternative tool that implements these capabilities, was designed, developed, and tested in a real operating scenario.

Keywords:
Security Auditing,
ISO/IEC27001,
Security management,
Strong access control,
Free software.

RESUMEN

La seguridad de la información es un aspecto fundamental de toda organización, no es exclusiva de empresas grandes; disponer de unas buenas prácticas en gestión de seguridad es relevante para ser competitivo en el contexto, sin embargo adoptar un estándar en este sentido, es un proceso tedioso y costoso para las empresas pequeñas. Las auditorias hacen parte de la adecuada gestión de la seguridad de información, ayudan a prevenir incidentes y también a mitigar riesgos sobre los activos de información. Muchas aplicaciones de este tipo, se desarrollan y ejecutan en escenarios tecnológicos privados o son costosas; no están disponibles para la comunidad y se enfocan en el funcionamiento, pero con serias dificultades en garantizar o documentar los servicios de confidencialidad y anonimato. Con este propósito se diseñó y desarrolló una herramienta alternativa denominada SANI; que implementa estas capacidades, las cuales fueron verificadas en un escenario real de operación.

Palabras clave:
Auditoría de seguridad,
ISO/IEC27001,
Gestión de la seguridad,
Control de acceso de fuerte,
Software libre.

[1] MSc. in Free Software, Professor, Faculty of Basic Sciences and Engineering, Universidad de los Llanos, Villavicencio, Colombia, E-mail: dfranco@unillanos.edu.co ORCID: https://orcid.org/0000-0002-6748-0729

[2] BSc. in Systems Engineering, Universidad de los Llanos, MSc. (c) in Systems and Computer Engineering. Universidad de los Llanos, Open Technologies Research Group - GITECX, Colombia. E-mail: hernan.porras@unillanos.edu.co ORCID: https://orcid.org/0000-0001-7015-1582

[3] MSc. in Free Software; area of network and operating system administration. Specialist in Telematic Solutions and Systems Engineer. Professor, Faculty of Basic Sciences and Engineering, Universidad de los Llanos, Villavicencio, Colombia. E-mail: felcorredor@unillanos.edu.co ORCID: https://orcid.org/0000-0002-3389-9951

[4] BSc. in Systems Engineering, Universidad de los Llanos. Open Technologies Research Group - GITECX, Colombia. E-mail: cristian.calderon@unillanos.edu.co ORCID: https://orcid.org/0000-0001-5390-9910

Cite this article as: D. C. Franco-Mora, H. O. Porras-Castro, F. A. Corredor-Chavarro, C. Calderón-Bogotá, "SANI: Assistant for Information Security Auditing on ISO/IEC 27001", Visión Electrónica, vol. 2, no. 2, Special edition, 2019. . https://doi.org/10.14483/issn.2248-4728

1. Introduction

Information security relates to any aspect associated to the protection of information or data contained in any media, whether digital or physical; it is related to all areas of an organization such as IT, human talent, etc.

There are systems oriented to the implementation of information security mechanisms for organizations, based on the PDCA cycle (Plan-Do-Check-Act), called Information Security Management Systems (ISMS). These are systems of processes organized and documented to implement and manage an organization's information security, seeking to maintain confidentiality, integrity and availability. However, as the information delivered (transmitted, processed and stored) by the organization to these systems, corresponds to sensitive information, it must be provided with security services that ensure proper authentication, access control and confidentiality.

In order for an organization to determine its security management state, there are several standards such as OSSTMM, COBIT and ISO/IEC27001, that establish management aspects to be considered, such as good practices and controls that, if well implemented, make it possible to comply with the established information security requirements. Our project assumed this problem for small and medium-sized companies within the regional context, designing and developing an alternative solution called SANI; which consists of a secure web system, under the OWASP standard, capable of assisting this type of organizations in the implementation of its ISMS.

This article presents the review of some tools in the context of security management; followed by the proposed architecture, where the different components of the exposed solution are explained, its implementation, the discussion of the results obtained from the design and the applied case, and finally, the conclusions collected.

2. Contextualization of the problem

Businesses today depend on their information assets and protecting them is a priority for their continuity [1], as computer attacks are increasing every day, on number, effectiveness, complexity and impact. Attacks generated by malware, phishing, ransomware, electronic fraud, among other threats, cannot be avoided, but companies can be prepared by means of an ISMS [2] integrated to a risk management system, as the basis of the methodological process, that provides controls and mitigation measures based on a security plan adjusted to the organizational processes [3-4].

According to the Pwc-2016 Information Security Global Report, more than a third (32%) of Colombian organizations declare having been victims of cybercrime and 76% suffered from misappropriation of assets [5]. This occurs due to the lack of good information security management, since only 33% of organizations have a response plan for cybercrime [5]. Most organizations are not prepared and do not even address the risks they face.

Many organizations are suffering information loss due to the lack of information security management; according to ACIS in its 2017 national information security survey, where 128 organizations from different fields participated, 29% of the respondents said they do not know if their organization manages security incidents, nor how that management is done [6-7].

In Colombia, some organizations use tools such as an information security system to prevent attacks [5],[8], but something more robust is needed. An information security management system (ISMS), being a fundamental aspect for any organization, implies creating a plan of design, implementation, and maintenance of a series of processes that allow efficient management of information assets, to assure their integrity, confidentiality and availability, in each organization [9-10].

The most widely used standard for information security management systems in Colombian organizations is ISO/IEC 27001:2013 with a 57% of usage; more than a half of the country's organizations use it for the definition of their security policies, moreover, there are 103 Colombian organizations with ISO/IEC 27001 certification [11]. Other similar standards used are ITIL (35%), COBIT 5 (24%) and the NIST guidelines (20%) [5]. In addition to the statistics mentioned, another reason why the ISO/IEC 27001 standard is the trend for security management, is that it is in line with the rest of security standards in the national context.

A 60% of Colombian organizations carry out internal audits to measure the level of security they possess and to determine vulnerabilities [12], [13]; for certification, companies carry out external audits. These external audits are conducted by specialized companies that determine the security level of the organization's ISMS. However, the cost of an audit is high and therefore there are companies (SMEs) or organizations that do not implement them, thus intruders could get into their information systems and attack on vulnerabilities without them noticing [2], [5], [7].

Based on the ISO/IEC 27001 standard, which describes the procedures used for information security management in an organization; a free-access and use, web-oriented tool was developed, with the purpose of allowing organizations to conduct internal audits in order to know their vulnerabilities and support risk management, and therefore, increase the chance of achieving certification during external audits [14-15]. The SANI tool, developed from this project, provides services of confidentiality, authentication and strong access control to generate trust in organizations about the treatment of sensitive data.

3. Methodological development

Table 1 below shows the support tools used for security management in organizations. Most of them are of proprietary type, and are used specifically within audit firms for their commercial activity.

Meycor COBIT Control Self - Assessment (CSA)	Software tool developed by DATASEC (http://nextpoint.com.do/web/?page_id=1331) with unique characteristics, since in its current version, worldwide standards such as the COBIT® 5.0 framework are incorporated.
GxSGSI - RISK ANALYSIS SO FTWARE	Developed by SIGEA, a company of Asturian origin, specialized in implementation consultancy and advice on systems based on ISO 27001, ISO 20000, ISO 28000, UNE 71599, SPICE, ICT Governance or the National Security Scheme (http://www.sigea.es/gap_27001.pdf). GxSGSI is a Risk analysis software developed in Visual Basic and supported under an SQL Server database, aimed at performing Security Risk Analysis necessary for the certification of an Information Security Management System, under the UNE 71502 and ISO 27001 standards. Country: Spain.
GlobalSGSI	GlobalSGSI developed by AUDISEC (http://audisec.es/index.php?option=com_content&view=article&id=30&Itemid=54), is an integral management web tool for the ISO 27001 standard. Country: Spain.
Secuware Security Framework (SSF)	Developed by SECUWARE, is a modular business suite used to protect an organization's information from problems such as virus, Trojans and other malicious codes, as well as for information access and platform usage control. Country: Spain.
Securia SGSI	Developed by the European Business and Innovation Centre of the Principality of Asturias (CEEI Asturias), sponsored by IDN Servicios Integrales, the Center of Excellence for Free Software, among others (http://www.binaryti.com/2012/02/securia-sgsi.html). It is free software but it is generic, not web oriented and its functionality is still limited.
E-Pulpo	Developed by Ingenia, an information technology, communications and Internet services company (https://ingenia.es/productos/epulpo/). E -Pulpo was born from a research that generated a software for the management of information security in organizations, both in the public administration and the private sectors: National Security Scheme (ENS), LOPD, SGSI (ISO 27001), etc. Country: Spain.
Excellence Suite (SE Suite)	Software tool developed by SoftExpert (https://www.softexpert.es/solucao/iso-27001/) which provides a comprehensive and advanced solution for information security management allowing organizations to meet the requirements of ISO 27001.
Gesttic - Software ISO	Developed by Gesttic (https://iso.cat/es/gesttic-software-iso/), it offers systematic risk - analysis of information security threats and vulnerabilities, as well as compliance with ISO/IEC 27001.
ISOTools	Developed by ISOTools (http://www.isotools.com.co/normas/ntc-iso-27001/) this tool allows organizations to comply with the requirements established by ISO/IEC 27001 and others, also meeting the controls defined by ISO 27002.

Table 1. Tools for information security management. Source: own.

3.1. Architectural Design

In the process of business, architecture and database modeling, two final semester students and an information security research engineer participated. The respective analysis of the system was carried out, thus defining the main functions and use cases as shown in "figure 1".

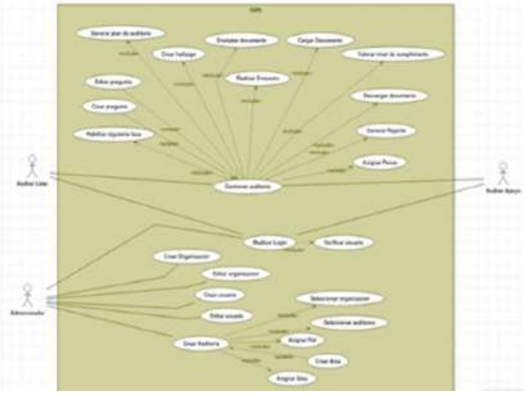


Figure 1. SANI, Overall Use Case. Source: own.

The design took into account the services of confidentiality, integrity and availability of data, including levels of access control. The SANI system was defined with an architecture that guarantees optimal operation and the possibility of expansion. The modules defined are shown below. See "Table 1".

Table 1. Description of SANI modules. Source: own.

Module	Description
Administration	Allows CRUD operations, for users, roles, audits, etc.
Inference	Allows the prediction of the weight of controls and the level of compliance that the organization should have to be audited; based on historical information stored in the database.
Reports	Allows to generate documents with information of the audit that is finalized, showing results and graphs that help to take decisions.
Authentication	Allows login based on a simple "user - password" method, with the guarantee that the passwords are really the ones registered in the system.
Communication	Allows the use of encrypted channel with HTTPS protocol, for information transfer.
Data Encryption	Allows the use of a suitable encryption algorithm for sensitive data such as authentication passwords and file contents.

Figure 2 shows the architecture design defined for SANI, including the coupling of each of the components and modules, representing some of the system functions

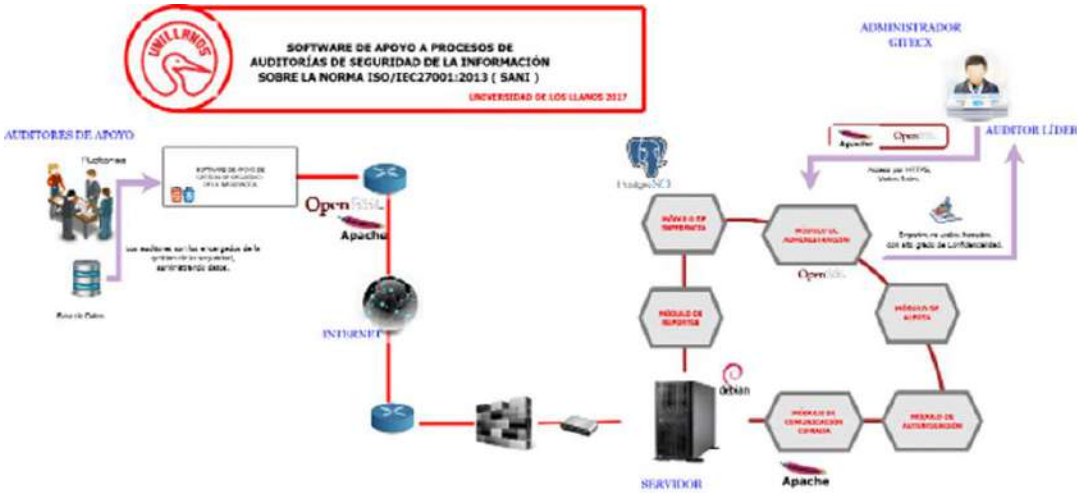

SOFTWARE DE APOYO A PROCESOS DE
AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN
SOBRE LA NORMA ISO/IEC27001:2013 (SANI)
UNIVERSIDAD DE LOS LLANOS 2017
UNILLANOS
AUDITORES DE APOYO
ADMINISTRADOR
GITECX
AUDITOR LÍDER
OpenSSL
Apache
INTERNET
PostgreSQL
debian
SERVIDOR
Apache

Figure 2. Architecture defined for the system – SANI. Source: own.

SANI was designed for a concurrence of three actors, which are described in "Table 2", including their levels of access to the system. The audit will be managed collaboratively, so that users involved in the process will have a dynamic participation.

Actor	Description
Administrator	The system administrator user, has specific tasks such as: the function to create all the parameters needed to start an audit. This user can participate in an audit as a lead or support auditor.
Lead Auditor	User that participates in the whole process of an active internal corporate audit. This user has the functions of uploading and downloading documentation, encrypting sensitive documentation, filling out checklists, recording findings, giving assessment to audit and generating reports.
Support Auditor	User who participates in the process of an internal corporate audit. This user is responsible for reviewing documentation of the organization and filling out assigned checklists to show corresponding findings.

Table 2. Actors in the SANI system. Source: own.

As information security is a priority in the project, modular integrated mechanisms were used to provide proper privacy and anonymity, including access control. These security mechanisms are described in Table 3

Module	**Description**
Login	Password encrypted with AES 256 in CBC mode of operation. OpenSSL library.
Encryption of confidential data	Sensitive data encrypted with AES 256 in CBC mode of operation, OpenSSL library.
HTTPS	Secure data transfer from system to user, in the application layer of the OSI Model.
Transactions and logs	Record of transactions and actions performed by system actors during each audit process.

Table 3. Security mechanisms. Source: own.

4. Implementation

The technological tools used such as, the development environment, programming language, libraries, web server, security mechanisms, databases, among others, are presented in "Table 4". These were selected according to the requirements defined in the phases and taking into account that their licensing is free software.

MODULE	TOOL	LICENSE	TYPE	DESCRIPTION
Authentication	PHP – OpenSSL – library.	Apache	Programming Language	Authentication passwords encrypted with AES 256 in CBC mode of operation .
Data Encryption	PHP – OpenSSL – library.	Apache	Programming Language	Module responsible for the encryption of sensitive data of the auditees (organizations).
Access Control	PHP	Apache	Programming Language	Use of roles to assign transactions and access controls.
Communication	OpenSSL	Apache	Library	Security layer applied for information exchange protection.
Inference	PHP	PHP	Programming Language	Algorithm for predicting weights and levels of compliance with controls in an audit process.

Table 4. Correlation of technologies with modules. Source: own.

4.1. Methodological process of the audit

As this project is based on the ISO/IEC 27001 standard, which does not establish how to carry out an audit process; the ISO 19011 standard was adopted for this purpose. Four phases were defined for the audit process, each one with its respective activities described in "Table 5".

Phase	Description
Start of the audit.	Determine the legal and contractual applicable requirements and other relevantrequirements for the activities and products of the audit.
Documentation review.	Review of missional documents, record of visit for general observations and weighting of audit controls.
Drafting of findings.	Audit sampling, generation of findings andaudit progress meetings. Finally, an assessment of compliance levels is given.
Audit conclusions.	Technical documents, preparation and distribution of audit reports (executive and technical) and audit closure.

Table 5. Phases of the Audit Process. Source: own

4.2. User interface

For the presentation and explanation of some of the SANI system processes, the most important of them are shown below, along with a brief description. For the assessment of controls during audits, SANI has a view where the description of each one is presented, allowing users to be correctly informed.

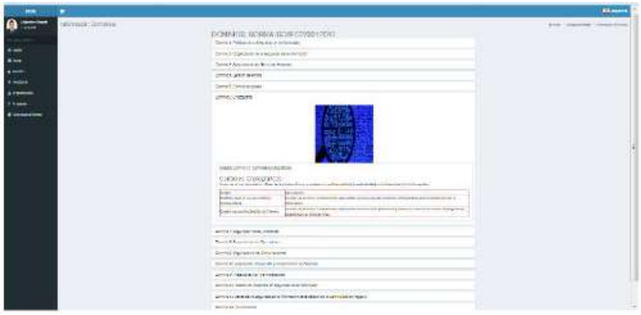


Figure 3. Information of Domains in SANI. Source: own.

When managing an audit, SANI allows to add a defined number of documents as needed in the different phases of each process and according to the role assigned.

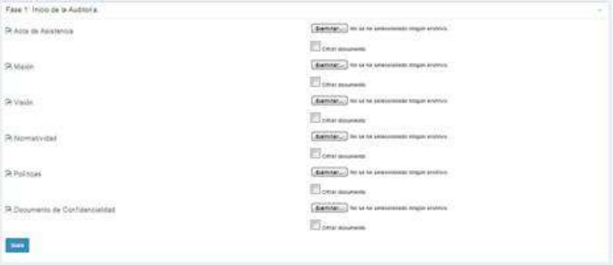


Figure 4. Document loading. Source: own.

Each auditor is provided with a view where they can observe all the audits in which they are participating, including the percentage of progress.

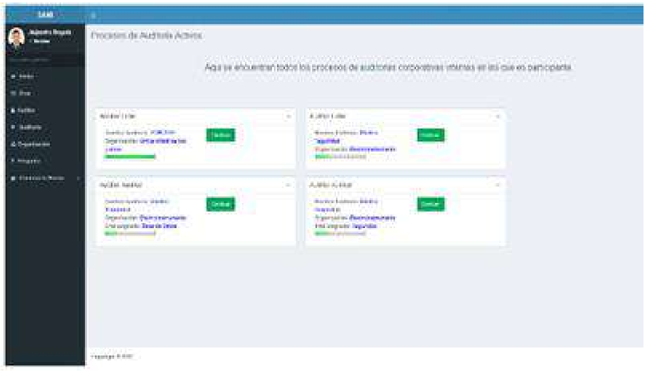

SANI
Procesos de Auditoría Activos
Aquí se encuentran todos los procesos de auditorías corporativas internas en las que es participante

Figure 5. Audit List. Source: own.

For the completion of each audit process, SANI will show some graphs created automatically when analyzing the assessment data in the audit, these graphs are exported in a report format for detailed explanation.

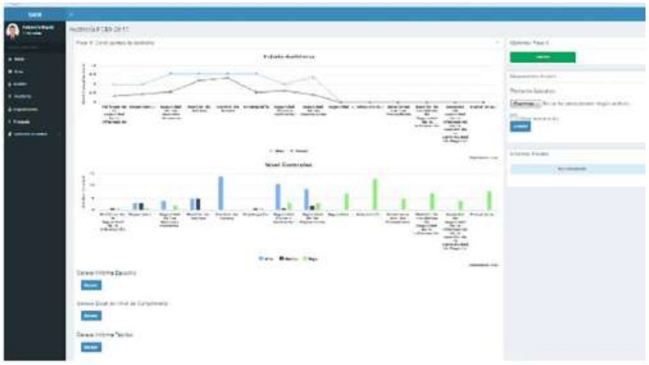
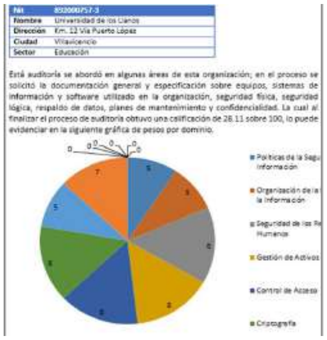


Figure 6. Graphics generated automatically by SANI. Source: own.

For the executive report, graphs of the current state and the initial state of the audited organization are taken into account, for the detailed report a table with the values of the audit assigned to it, and for the technical report the description of the entire audit process conducted and its results.

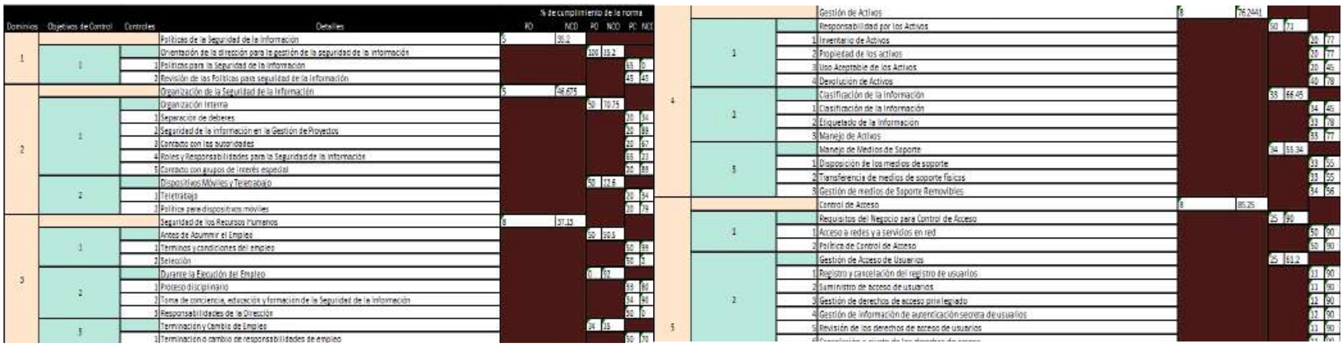


Nit	892000757-3
Nombre	Universidad de los Llanos
Dirección	Km. 12 Vía Puerto López
Ciudad	Villavicencio
Sector	Educación

Está auditoría se abordó en algunas áreas de esta organización; en el proceso se solicitó la documentación general y especificación sobre equipos, sistemas de información y software utilizado en la organización, seguridad física, seguridad lógica, respaldo de datos, planes de mantenimiento y confidencialidad. La cual al finalizar el proceso de auditoría obtuvo una calificación de 28.11 sobre 100, lo puede evidenciar en la siguiente gráfica de pesos por dominio.

0
0
0
0
0
0
5
5
6
8
8
8
5
7
Políticas de la Segu información
Organización de la la información
Seguridad de los Re Humanos
Gestión de Activos
Control de Acceso
Criptografía

Figure 7. Executive Report generated by SANI. Source: own.



Dominios	Objetivos de Control	Controles	Detalles	% de cumplimiento de la norma PD	NCD	PO	NCO	PC	NCC
1			Políticas de la Seguridad de la Información	5	30.2				
	1		Orientación de la dirección para la gestión de la seguridad de la información			100	15.2		
		1	Políticas para la Seguridad de la Información					65	0
		2	Revisión de las Políticas para seguridad de la información					45	45
2			Organización de la Seguridad de la Información	5	46.675				
	1		Organización Interna			50	70.75		
		1	Separación de deberes					20	34
		2	Seguridad de la información en la Gestión de Proyectos					20	89
		3	Contacto con las autoridades					20	67
		4	Roles y Responsabilidades para la Seguridad de la Información					65	23
		5	Contacto con grupos de interés especial					20	88
	2		Dispositivos Móviles y Teletrabajo			50	12.6		
		1	Teletrabajo					20	34
		2	Política para dispositivos móviles					20	79
3			Seguridad de los Recursos Humanos	8	37.15				
	1		Antes de Asumir el Empleo			50	50.5		
		1	Términos y condiciones del empleo					50	99
		2	Selección					50	2
	2		Durante la Ejecución del Empleo			0	92		
		1	Proceso disciplinario					33	80
		2	Toma de conciencia, educación y formación de la Seguridad de la Información					34	90
		3	Responsabilidades de la Dirección					50	0
	3		Terminación y Cambio de Empleo			24	15		
		1	Terminación o cambio de responsabilidades de empleo					50	70
4			Gestión de Activos	8	76.2441				
	1		Responsabilidad por los Activos			50	71		
		1	Inventario de Activos					20	77
		2	Propiedad de los activos					20	77
		3	Uso Aceptable de los Activos					20	45
		4	Devolución de Activos					40	78
	2		Clasificación de la Información			33	66.45		
		1	Clasificación de la Información					34	45
		2	Etiquetado de la Información					33	78
		3	Manejo de Activos					33	77
	3		Manejo de Medios de Soporte			34	55.34		
		1	Disposición de los medios de soporte					33	55
		2	Transferencia de medios de soporte físicos					33	55
		3	Gestión de medios de Soporte Removibles					34	56
5			Control de Acceso	8	85.25				
	1		Requisitos del Negocio para Control de Acceso			25	90		
		1	Acceso a redes y a servicios en red					50	90
		2	Política de Control de Acceso					50	90
	2		Gestión de Acceso de Usuarios			25	61.2		
		1	Registro y cancelación del registro de usuarios					11	90
		2	Suministro de acceso de usuarios					11	90
		3	Gestión de derechos de acceso privilegiado					12	90
		4	Gestión de información de autenticación secreta de usuarios					12	90
		5	Revisión de los derechos de acceso de usuarios					11	90
		6	Cancelación o ajuste de los derechos de acceso					11	90

Figure 8. Detailed Score Report. Source: own.

5. Discussion

This section deals with the case study of the audit process of the Faculty of Basic Sciences and Engineering "FCBI" of the University of the Llanos. This faculty has 11 dependencies, of which 4 were taken into account in the audit test case.

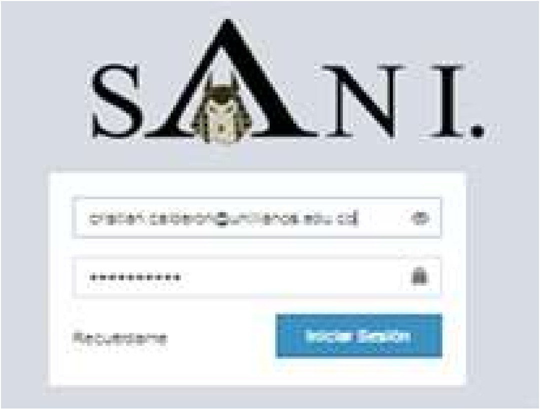
Dependence	Information Assets	Regulation	Risks
Deanship	1. Institutional access credentials 2. Correspondence 3. Curriculum vitae 4. Agreements	1. Superior Agreement 012 of 2009 2. Superior Agreement 004 of 2009	1. Spoofing 2. Institutional disrepute 3. Lost profit
Academic secretariat	1. Council acts. 2. Access credentials. 3. Teacher evaluation reports.	1. Superior Agreement 012 e 2009 2. Superior Agreement 004 of 2009	1. Spoofing 2. Institutional disrepute 3. Lost profit
Department of Mathematics and Physics	1. SARA system access credentials 2. Teachers' resumes	1. Superior Agreement 012 e 2009 2. Superior Agreement 004 of 2009	1. Spoofing 2. Fraud 3. Denial of service
Social projection	1. Convention blogs 2. Graduate information 3. Credentials	1. Superior Agreement 021 of 2002 2. Superior Agreement 004 of 2009 3. Superior Agreement 012 of 2009	1. Theft 2. Fraud 3. Denial of service 4. Spoofing

Table 6. FCBI dependencies, in the test case. Source: own

These units were audited in the area of security, databases and operating systems; for the assessment, Annex A of the ISO/IEC 27701:2013 standard was taken into account, with a list of 114 controls that make up 14 domains, where cryptography was given 18% priority, 15% priority for physical and environmental security, and 10% priority for operational security.

For this audit process, three student-type users, belonging to the GITECX research group and an expert engineer in information security, were created through the SANI interface.

The SANI system was equipped with a secure and encrypted authentication system with security protocols for sending information.



cristian.calderon@unillanos.edu.co

•••••••••••

Figure 9. SANI authentication module. Source: own.

The system was installed in 3 computers of the Gitecx research group laboratory, in which the audit process was carried out for the FCBI dependencies.

Once the audit is created, the lead auditor assigns the assistants who will participate in the audit, starting the audit plan.

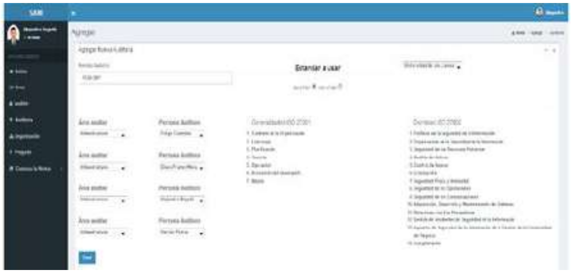
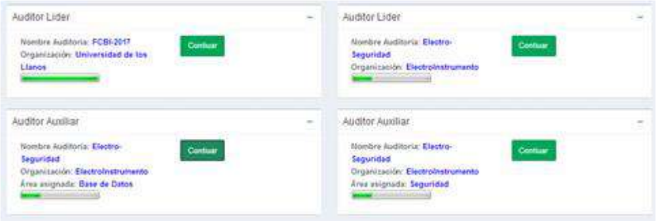


Figure 10. Audit creation. Source: own.

The functionality of the SANI system was verified by comparing each result of the values of the audit compliance levels. A brief analysis of the reports generated by the system from its interface, was made.



Auditor Lider
Nombre Auditoria: FCBI-2017
Organización: Universidad de los Llanos

Auditor Lider
Nombre Auditoria: Electro-Seguridad
Organización: ElectroInstrumento

Auditor Auxiliar
Nombre Auditoria: Electro-Seguridad
Organización: ElectroInstrumento
Área asignada: Base de Datos

Auditor Auxiliar
Nombre Auditoria: Electro-Seguridad
Organización: ElectroInstrumento
Área asignada: Seguridad

Figure 11. Audit access and progress. Source: own.

An intuitive user interface, which allows to carry out the entire assigned audit process was implemented for the SANI system. Security mechanisms were incorporated, focusing on encryption of credentials and sensitive data, as well as functional aspects for the analysis of results and graphic reports with statistical details.

5.1. Deployment of SANI security mechanisms

In this section, the application security level is analyzed, based on the Open Web Application Security Project (OWASP).

Currently, cybersecurity is an important axis in any organization, information is considered an asset and applications are used to process it. Information assets are susceptible to the most critical security risks already present in the context. Based on this approach, the SANI analysis was performed, within the framework of the "OWASP top ten Project", as the data (Security Audit Results) stored, transmitted and processed by SANI, is considered critical and sensitive data, an active valuable to any organization.

OWASP 2017	Compliance
Injection	The SANI system has a control of supported characters for each field validated by the server. Likewise, the application does not contain dynamic scripts so the user does not have to enter data to consult directly in the database, greatly reducing SQL data injection.
Broken authentication	SANI has a token system with a lifetime in case of inactivity, this system is based on AES-256 encryption and is provided by the Laravel framework.
Sensitive data Exposure	The most critical data found in the system, such as findings, security policies, meeting attendees, etc., is encrypted on the server. In case of physical theft, this data cannot be read.
XML External Entities (XXE)	
Broken Access Control	The system has a token so that access control cannot be lost, which immediately warns any system error.
Security Misconfiguration	SANI is hosted in an application server with the respective firewall rules associated, as well as other security measures, such as redirection to the database, prohibition of ICMP type 8 traffic entrance, IDS and WAF modsecurity.
Using Components with Known Vulnerabilities	The system has the minimum of extra components, stable version control is maintained in each one of the applications.
Insufficient Logging & Monitoring	The system has a log mechanism for each transaction carried out in the application. Moreover, the web logs analyzer "webalizer" was configured.

Table 7. OWASP compliance. Source: own.

6. Conclusions

SANI is an audit process assistance tool, which includes internal confidentiality modules for the treatment of sensitive data needed during and after each audit. These data are information assets with high risk for business continuity in the event of loss of confidentiality, anonymity or access control. For this reason, the guidelines of the OWASP project are strictly necessary for the construction of applications used in cybersecurity.

Support applications for information security management are developed and executed in private technological scenarios by companies dedicated to providing these services. They are not available to community and those that exist, focus on functionality but have serious problems in guaranteeing confidentiality and anonymity services (due to poor cryptographic capabilities), for this reason SANI is an added-value alternative that implements these capabilities. Other applications for security auditing, [16-19]

Acknowledgments

The authors express their gratitude to God and their families, who have always supported this process. Likewise, to the Universidad of the Llanos for believing in this research project called "Methodological assistant for the implementation of information security audits on ISO/IEC 27001 (C01-F02-006-2016)" and financing it completely.

References

[1] A. Solano, "La voz del CISO. Directores de seguridad de la información responden cuatro preguntas clave dentro de su gestión.," 2015.

[2] A. R. Almanza Junco, "Tendencias 2016. Encuesta nacional de seguridad informática", SISTEMAS, pp. 18-37, 2016.

[3] B. Barafort, A.-L. Mesquida, and A. Mas, "Integrating risk management in IT settings from ISO standards and management systems perspectives," *Comput. Stand. Interfaces*, vol. 54, pp. 176-185, Nov. 2017. https://doi.org/10.1016/j.csi.2016.11.010

[4] B. Barafort, A. L. Mesquida, and A. Mas, "Integrated risk management process assessment model for IT organizations based on ISO 31000 in an ISO multi-standards context," *Comput. Stand. Interfaces*, vol. 60, pp. 57-66, Nov. 2018. https://doi.org/10.1016/j.csi.2018.04.010

[5] E. D. Econ, "Hacia una nueva ética en los negocios: preparados para evitar el crímen económico y cibernético," 2016.

[6] ACIS, "VIII Encuesta Latinoamericana de Seguridad de la Información Nuevos horizontes para América Latina Jeimy J. Cano M., Ph.D, CFE Gabriela María Saucedo Meza, MDOH," 2016.

[7] J. J. C. M, D. Ph, G. María, S. Meza, and D. Ph, "Ix informe de encuesta latinoamericana de seguridad de la información," no. c, pp. 1-10, 2017.

[8] K. V. Urbina and J. S. Suárez, "AUDITORIA DE SISTEMAS. EMPRESAS DE AUDITORIA EN COLOMBIA," 2014, p. 8.

[9] N. T. Ntc-iso-iec, Norma técnica ntc-iso-iec colombiana 27001 2013-12-11, no. 571. 2013.

[10] F. Dumont, S. Jemai, Z. Xu, P. M. Felan, and G. Farges, "Sécurité de l'information : autodiagnostic selon l'ISO/CEI 27001," IRBM News, vol. 39, no. 4-5, pp. 90-95, Oct. 2018. https://doi.org/10.1016/j.irbmnw.2018.08.001

[11] "The ISO Survey," certificaciones ISO 27001 Mundial.

[12] C. Merino Bada and R. Cañizares Sales, Implantación de un sistema de gestión de seguridad de la información según ISO 27001: Un enfoque práctico. FC editorial, 2011.

[13] Trend Micro and Oea, "Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas," 2015.

[14] L. Qi, D. Qingling, S. Wei, and Z. Jine,

Measurement Model under Four Clusters Standards (ISO 9001, 14001, 27001, OHSAS 18001)," Procedia Eng., vol. 37, pp. 354-358, Jan. 2012. https://doi.org/10.1016/j.proeng.2012.04.252

[15] N. V. Syreyshchikova, D. Y. Pimenov, and T. Mikolajczyk, "Information Safety Process Development According to ISO 27001 for an Industrial Enterprise," Procedia Manuf., vol. 32, pp. 278–285, Jan. 2019.

[16] O. Ospina Zuñiga, G. García Cobas, J. Gordillo Rivera and K. Tovar Hernández, "Assessment of Murky Water and its Conductivity During Dry and Rainy Seasons in Combeima River (Ibagué, Colombia)", Ingeniería Solidaria, vol. 12, no. 19, pp. 19-36, 2016. https://doi.org/10.16925/in.v12i19.1191

[17] J. A. Vargas, J. Arango and L. G. Isaza Domínguez, "Instructional Strategy to Train Professors from the Civil Engineering Program in the Use of Information and Communications Technologies (ICTS) at the Villavicencio Campus of the Universidad Cooperativa de Colombia", Ingeniería Solidaria, vol. 10, no. 17, pp. 161-174, 2014. https://doi.org/10.16925/in.v9i17.829

[18] E. Campero, "Productive Chains as a Source of Opportunities for Entrepreneurs in the Rural Sphere", Ingeniería Solidaria, vol. 11, no. 18, pp. 75-85, 2015. https://doi.org/10.16925/in.v11i18.993

[19] A. P. Becerra Quiroz, A. L. Buitrago Coca and P. Pinto Baquero, "Sustainability of sugar cane bagasse utilization in Valle del Cauca, Colombia", Ingeniería Solidaria, vol. 12, no. 20, pp. 133-149, 2016. https://doi.org/10.16925/in.v12i20.1548

[20] L.Y. Gualdrón - Prieto, J.M. Acosta - Romero and L.E. Bohórquez - Arevalo, "Organizational structures and adaptation to changing environmental conditions Challenges and implications". Ingeniería Solidaria,Vol. 13, No. 23. pp 115-117. https://doi.org/10.16925/in.v23i13.1983