SOFTWARE DE APOYO A PROCESOS DE AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN SOBRE LA NORMA ISO/IEC27001:2013 (SANI)

HERNÁN OSWALDO PORRAS CASTRO 160002827

CRISTIAN ALEJANDRO CALDERÓN BOGOTÁ 160002806

UNIVERSIDAD DE LOS LLANOS

FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA

ESCUELA DE INGENIERÍAS

PROGRAMA DE INGENIERÍA DE SISTEMAS

VILLAVICENCIO, COLOMBIA

2017

SOFTWARE DE APOYO A PROCESOS DE AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN SOBRE LA NORMA ISO/IEC27001:2013 (SANI)

HERNÁN OSWALDO PORRAS CASTRO 160002827

CRISTIAN ALEJANDRO CALDERÓN BOGOTÁ 160002806

Directora:

DIANA FRANCO MORA M.Sc

Codirector:

FELIPE CORREDOR CHAVARRO M.Sc

UNIVERSIDAD DE LOS LLANOS

FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA

ESCUELA DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

VILLAVICENCIO, COLOMBIA

2017

NOTAS DE ACEPTACIÓN:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____
DIANA FRANCO MORA

Directora

_____
FELIPE CORREDOR

Codirector

_____
Jurado

_____
Jurado

_____
Fecha

AGRADECIMIENTOS

En primera instancia agradezco a mi padre Edgar Porras y mi madre Inés Castro, mis hermanas, hermano y mi familia aquí en Villavicencio, que durante todo el proceso de mi formación me estuvieron apoyándome. Ellos que me vieron seguir noches enteras para entregar trabajos y seguir con cabeza en alto.

A mis maestros y secretarias que sin ellos no podría llegar a ser el profesional que soy ahorita, ellos que dedicaron su tiempo a enseñarme, defenderme en un mundo laboral y formarme como persona. También a los miembros del comité de Investigaciones gracias a ustedes aprendí mucho y me ayudaron a fortalecerme, Mónica Quiceno, Ángel Cruz, Miguel Navarro, Cesar Díaz, Hernando Ramírez y Javier Martínez.

A mis compañeros, los cuales pasamos tiempos felices y amargos. Ellos que estuvimos compartiendo tiempos de baile, fiesta, estudio, entre otras. Ellos que por muchas noches que seguimos en vela sin dormir estuvieron allí apoyándome en todo momento, menciono a algunos Cristian Calderón, Christian Galvis, John Alex, Camilo Barrera, Fabián Barrios, Oscar Pedraza (aunque salió de la U), entre otros.

Al grupo de investigación GITECX, este grupo que desde un comienzo tuvo la disposición de ayudarnos en el proceso de graduación, prestando todos sus materiales y apoyo de cada uno de los profesionales pertenecientes, que me ayudaron a fortalecer cada una de mis falencias. A mis directores Felipe Corredor y Diana Franco, ellos quienes tuvieron la paciencia para aguantarnos en la demora, además de estar ayudando en el proceso y sus sabias palabras al momento de pedir un consejo.

Al grupo SISTEMAS DINÁMICOS, el grupo el cual empecé mi formación como investigador y enseñanzas. Al profesor Jesús Arias, quien en todo momento me apoyo en mi proceso, el quien me dio unos consejos que no olvidare. El quién sacrifico sus días sábados para seguir con el proyecto de simulación, gracias profe por todo el apoyo y por ser esa persona quien me ayudo hacer un profesional y apoyarme en no dejar mis sueños votados.

A una gran amiga que se fue de la ciudad, ella que por más que me guste molestarlas y no hablamos como antes, pero ha estado conmigo de forma lejana o eso pienso. Ella quien me enseño mucho de la vida le agradezco. A mis otras amigas, quienes siempre me regañaron por ser tan descuidado gracias por sus concejos. Mónica Soracá, Bárbara Camargo, Karen Álvarez, Andrea Valbuena (ojitos, una ternura de mujer), entre otras. A ellas gracias por estar conmigo y aguantar mi forma de ser en serio se merecen que ponga esto aquí (sobre todo

Bárbara Camargo, disculpa por sacarte tanto mal genio, pero es muy entretenido verte en todos tus estados de humor gracias Ingeniera).

A Iron Fuentes, Oscar Collazos, Kevin Acosta y Julián Garzón, amigos de Bogotá los cuales en todas las vacaciones me esperan para salir con ellos y recordar los tiempos de colegio. Quiero dedicarles esta parte y decirles MUCHACHOS ESTOY TRIUNFANDO. También a sus familias claro está.

A Cristian Calderón, el quien fue mi amigo y compañero de Tesis le agradezco por tenerme paciencia a la hora de hacer la tesis y trabajos. Perdón por hacerlo pasar noches en vela y torturarlo con la programación (espero me perdone en serio que lo torture con trabajos), solo espero que siga el bueno amigo que es y que siga caminando hacia adelante que puede contar conmigo para lo que necesite.

A las amigas de colegio Lorena y Marcela soler por siempre esperarme en vacaciones y recibirme con tanta alegría gracias. También a Andrea Castro, Lida Castro y su familia, quienes el poco tiempo que estaba con ellos me hicieron pasar momentos muy agradables.

Finalmente, me gustaría mencionar a otros amigos los cuales pase muchas cosas con ellos, pero el papel no alcanza, sin decir más agradezco a la Universidad de los llanos, esta entidad la cual pase seis años en proceso de formación y me dio mucho. Gracias de todo corazón y es un honor ser UNILLANISTA.

HERNÁN OSWALDO PORRAS CASTRO

AGRADECIMIENTOS

Doy gracias a Dios por permitirme estudiar en una universidad, pues no lo tenía pensado en mi vida y más culminar una carrera la cual es para personas que tienen ingenio para dar solución a cualquier problema.

Gracias a Dios por permitirme tener unos padres los que con sus consejos me ayudaron día a día seguir adelante, mi madre María Bogotá motor de mi vida a la que con mi vida la amo y me dio esa fuerza y el ejemplo de salir con una carrera, mi padre Carlos Calderón y mi tío Henry Calderón que con historias me dieron a entender que no todo es fácil pero que con firmeza y responsabilidad se puede lograr muchas cosas.

Gracias a Dios por permitirme conocer a personas que contribuyeron en mi vida académica, Hernán Porras gran amigo que me ayudo bastante en muchas materias, y los amigos de la carrera que también con alegrías y angustias pasamos muchas de las duras materias. También a los integrantes del grupo GITECX que nos ayudaron en el proceso de este trabajo.

CRISTIAN ALEJANDRO CALDERÓN BOGOTÁ

ÍNDICE DE CONTENIDO

CAPITULO 1.

1. RESUMEN

El informe que se presenta a continuación tiene como fin contextualizar sobre los aspectos más importantes que se llevaron a cabo para la elaboración y puesta en marcha del SOFTWARE DE APOYO A PROCESOS DE AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN SOBRE LA NORMA ISO/IEC27001:2013. Usted podrá tener una visión panorámica del trabajo realizado en el desarrollo de esta herramienta web, la cual tiene como fin mostrar que nivel de seguridad tiene la organización referente a la gestión de la seguridad de la información, analizando los datos obtenidos en el proceso de auditoría.

La seguridad es parte fundamental de toda organización independiente de su tamaño y en la actualidad estar certificado en la parte de su gestión es tendencia, pues involucra a todos los procesos de las dependencias de una organización, pero una certificación es costosa y no todos puede acceder a ella, y las que tienen la forma corren el riesgo de perder su dinero. Para evitar gastos y prevenir posibles accidentes en la seguridad de la información se desarrolló una herramienta de software libre la cual ayuda a realizar procesos de auditoría corporativa interna basada en la norma ISO/IEC27001:2013 la que está actualmente rigiendo para la parte de gestión de seguridad, realizando listas de chequeo y análisis de resultados, el sistema es asequible a cualquier organización de forma segura con acceso fuerte y confidencialidad de la información sensible, pues la iniciativa de la herramienta es que en la región las organizaciones se motiven a lograr la certificación de la gestión de la seguridad.

Palabras clave: *Auditoría, ISO/IEC27001:2013, gestión de la seguridad, control de acceso de fuerte, software libre.*

2. ABSTRACT

The report presented below is intended to contextualize about the most important aspects that were carried out for the development and implementation of SUPPORT SOFTWARE FOR INFORMATION SAFETY AUDITS WITH STANDARDS ISO/IEC27001:2013. You can have a panoramic view of the work done in the development of this web tool, which aims to show the level of security of the organization regarding the management of information security, analyzing the data obtained in the audit process.

The security is a fundamental part of any organization independent of its size and currently being certified in the part of its management is trend, because it involves all the processes of the dependencies of an organization, but a certification is expensive and not everyone can access to her, and those who have the form run the risk of losing their money. In order to avoid expenses and prevent possible accidents in information security, a free software tool was developed which helps to carry out internal corporate audit processes based on the ISO / IEC27001: 2013 standard which is currently governing the management part of Security, performing checklists and analysis of results, the system is affordable to any organization in a secure way with strong access and confidentiality of sensitive information, since the initiative of the tool is that in the region organizations are motivated to achieve certification Of security management.

Keywords: *Audit, ISO / IEC27001: 2013, security management, strong access control, free software.*

3. PLANTEAMIENTO DEL PROBLEMA

La seguridad de la información en una empresa es parte clave para su continuidad, ya que éste bien intangible se debe proteger de diversos ataques informáticos[1]. Según el Informe Global de Seguridad de la Información de Pwc-2016 más de una tercia parte (32%) de las organizaciones de Colombia reportan haber sido víctimas de crimen cibernético y un 76% sufrieron de apropiación indebida de activos, esto se da porque no se hace un buen manejo de seguridad de la información, pues tan solo un 33% de las organizaciones tienen un plan de respuestas ante un ciber-crimen [2]. Esto nos dice que la mayoría de las organizaciones no están preparadas y ni siquiera no atienden a los riesgos que se enfrentan.

Muchas de las organizaciones están sufriendo perdidas de la información debido a que no tienen un manejo, una gestión de seguridad de la información; según el ACIS en su encuesta nacional de seguridad de la información donde participaron 128 organizaciones de distintos enfoques, para el 2017 el 29% de los encuestados dicen no saber si la organización maneja sus incidentes o cómo los maneja [3], [4].

Según F. Corredor en la región Orinoquía hay empresas de diferente enfoque, que manejan un sistema de seguridad de la información donde se previene de ataques[5], pero se necesita algo más robusto; un sistema de gestión de seguridad de la información (SGSI), siendo un aspecto fundamental para cualquier empresa, implicando crear un plan de diseño, implementación, y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente los activos de información, para asegurar la integridad, confidencialidad y disponibilidad de la misma, en cada una de las empresas de la región [6].

Las empresas, para medir el nivel de seguridad que poseen, realizan auditorías internas que les permitan determinan vulnerabilidades; y con el fin de obtener una certificación, realizan auditorías externas.

Estas auditorías externas son realizadas por empresas u organizaciones especializadas que determinan el nivel de seguridad del SGSI de la empresa. Sin embargo, el costo de una auditoría es muy elevado y por lo tanto hay empresas (PyMEs) u organizaciones que no lo realizan, por lo tanto ingresan intrusos a su sistema de información y hurtan información confidencial[5].

El estándar más usado para los sistemas de gestión de seguridad de la información en las organizaciones colombianas es la ISO/IEC 27001:2013 con un 57%, y el 55% de las organizaciones la usan para la definición de sus políticas de seguridad, existen 103 organizaciones colombianas con certificación ISO/IEC 27001[7]. Otros estándares que se usan similares a este son ITIL con un 35%, COBIT5 con un 24% y las guías del NIST el 20% [2]. Como referencia a las cifras anteriores se sabe que el estándar que es tendencia para la gestión de seguridad es ISO/IEC 27001, ya que esta se acopla a las demás normas de seguridad nacional.

Basados en el estándar ISO/IEC 27001, que describe cómo gestionar la seguridad de la información en una organización y/o empresa; se realiza el desarrollo de una herramienta, orientada a la web, de libre acceso y uso, que le facilite a las organizaciones de la región la realización de auditorías corporativas internas con el fin de conocer sus vulnerabilidades y así lograr una certificación. La herramienta tendrá un servicio de confidencialidad y control de acceso fuerte para que las organizaciones no teman por su información.

4. JUSTIFICACIÓN

Desde el área de teleinformática y el curso de seguridad informática en la Universidad de los Llanos, estudiantes han realizado estudios sobre la seguridad de la información en diferentes empresas de la región; basándose en la norma ISO/IEC 27001:2013.

Estudios que se han realizado como proyecto final de semestre, simulando auditorías internas. Pero los estudiantes no utilizan herramienta alguna para llevar a cabo este proceso, únicamente se apoyan de una hoja de cálculo que facilita en algo ese trabajo; ya que el uso de alguna herramienta de las existentes en el mercado, implica costos elevados que la Universidad no puede asumir.

Lo anterior debido a que la mayoría de herramientas de software para seguridad que existen son propias de firmas de auditoría, son restringidas y costosas, son difíciles de configurar/administrar, están muy relacionadas con la plataforma operativa, son genéricas, con restricciones de idioma, sin la documentación, ni acceso a los códigos fuentes, ni enfocadas al tipo de organización[8]. Y es por esta misma razón que las empresas no brindan la suficiente información para realizar un mejor proceso de auditoría, ya que consideran que no hay garantías con la confidencialidad de la misma.

El desarrollo de una solución con software libre, orientada a la web, como herramienta de apoyo para asistir metodológicamente cada proceso de auditoría corporativa interna; ofreciendo seguridad y confidencialidad en la información; es una buena alternativa para que las empresas puedan ejercer un mayor control en la seguridad de la información que administran.

5. OBJETIVOS

5.1. OBJETIVO GENERAL.

Desarrollar un software web de asistente metodológico para la implementación de auditorías corporativas internas de seguridad de la información sobre la norma ISO/IEC27001:2013.

5.2. OBJETIVOS ESPECÍFICOS.

- Desarrollar el diseño y codificación de los módulos de autenticación, de control de acceso, de inferencia, reportes, y gestión en general, propuestos por el grupo GITECX.

- Someter a pruebas el sistema en escenarios adecuados a las condiciones reales para refinar su funcionalidad.

- Elaborar documentación técnica y de usuario final de los módulos de software desarrollados.

- Realizar un estudio de contexto sobre los sistemas de apoyo a la implementación de ISO27001 y su impacto en el ámbito global, nacional y regional.

6. MARCO TEÓRICO

Las empresas según su índole deben establecer programas de seguridad enfocados en sus procesos de negocio, pues deben tener en cuenta que deben proteger su sistema de información de diferentes amenazas tecnológicas a la seguridad, como lo son el espionaje industrial, hurto de información, denegación de servicio, virus informático, entre otros, pues la información se ha convertido en el activo más importante y como cualquier activo importante necesita una protección especial[1]. De hecho, la información debe ser protegida adecuadamente con independencia de su formato o modo de transmisión[5][9][10]; la implantación de estándares de gestión de la seguridad de la información se ha convertido en una prioridad de las organizaciones para asegurar su continuidad, minimizando posibles daños, y ataques y maximizando el retorno de la inversión, oportunidades de negocio [6].

Aún no se tiene un gran impacto con los sistemas de gestión de seguridad de la información, porque algunas organizaciones no tienen idea de lo que pueden lograr con este [11]; el tener un SGSI e incluyendo una política de seguridad de la información como base necesaria para la realización de programas de seguridad se puede lograr la mitigación de riesgos de seguridad.

Existen estándares de SGSI a nivel internacional, modelos para buenas prácticas de seguridad, algunos como:

- La Norma ISO/IEC 27001:2013, es una norma estándar de seguridad que para su certificación se necesita cumplir sus criterios establecidos, este estándar se realizó por un arduo estudio en diferentes organizaciones de varios países, así determinar sus criterios[6].

- Information Security Management Maturity Model (ISM3), conocida como ISM-cubed o ISM3, está construido en estándares como ITIL, ISO

20000, ISO 9001, CMM, ISO/IEC 27001, e información general de conceptos de seguridad de los gobiernos. ISM3 puede ser usado como plantilla para un ISO 9001 compliant. Mientras que la ISO/IEC 27001 está basada en controles. ISM3 está basada en proceso e incluye métricas de proceso (http://www.lean.org/FuseTalk/Forum/Attachments/ISM3_v2.00-HandBook.pdf).

- SOGP, otro SGSI que compite en el mercado es el llamado "Information Security Forum's Standard of Good Practice". Este SGSI es más una "best practice" (buenas prácticas), basado en las experiencias del ISF (https://www.uninett.no/webfm_send/730).

- COBIT, Control Objectives for Information and Related Technology y es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA), y el Instituto de Administración de las Tecnologías de la Información (ITGI) en 1992 (http://goo.gl/ce7OjV).

El 60% de las organizaciones colombianas, para medir el nivel de seguridad que poseen, realizan auditorías internas que les permitan determinan vulnerabilidades [9], [12]; y con el fin de obtener una certificación, realizan auditorías externas. Estas auditorías externas son realizadas por empresas u organizaciones especializadas que determinan el nivel de seguridad del SGSI de la organización. Sin embargo, el costo de una auditoría es muy elevado y por lo tanto hay empresas (Pymes) u organizaciones que no lo realizan, por lo tanto ingresan intrusos a su sistema de información y pueden atacar en las vulnerabilidades del sistema y sin que ellos se den cuenta [2], [4], [11].

En Colombia se ha logrado obtener certificaciones de la norma ISO/IEC 27001:2013 desde el 2006, según ISO Survey y para el 2015 se logró 103 certificaciones, claro para alcanzar esta certificación también se debe tener en cuenta los controles que se manejan en la norma ISO/IEC 27002, pues son los controles que requiere la organización después de una validación con la declaración de aplicabilidad.

7. METODOLOGÍA

Se propuso usar como metodología RUP, enfocándose hacia un proceso investigativo donde se trazaron unos objetivos en el desarrollo de cada fase. Esto debido a que SANI es un sistema con módulos orientados a la web. Este proceso metodológico que se escogió consta de las siguientes fases:

7.1. FASE INICIAL

Esta fase sólo dispuso de una iteración, a continuación, desglosan las actividades y resultados atinentes a esta fase:

Actividades.

- Se inició con la definición de actores del sistema y recolección de requisitos funcionales y no funcionales:
  - Se definió los actores que participarán en el sistema.

NOMBRE	Administrador
DESCRIPCIÓN	Usuario administrador del sistema, tiene tareas específicas tales como: como función el crear todos los parámetros que se necesita para iniciar una auditoría. Este puede participar en una auditoria como auditor líder o de apoyo.

Tabla 1. Perfil Administrador del sistema.
Fuente: Autores

NOMBRE	Auditor Líder
DESCRIPCIÓN	Usuario que participa en todo el proceso de una auditoría corporativa interna activa. Este tiene la función de carga y descarga documentación, cifrar documentación sensible, llenar listas de chequeo, encontrar hallazgos, dar

	valoración a la auditoria y generar informes.

Tabla 1. Perfil Auditor líder.
Fuente: Autores

NOMBRE	Auditor de Apoyo
DESCRIPCIÓN	Usuario que participa en el proceso de una auditoría corporativa interna. Este se encarga de revisar documentación de la organización y llenar las listas de chequeo que se le asigna y con estas mostrar hallazgos.

Tabla 3. Perfil Auditor de apoyo.
Fuente: Autores

- Se definió los requerimientos funcionales y no funcionales del sistema.

MODULO	NOMBRE	IDENTIFICADOR	DESCRIPCIÓN
AUTENTICACIÓN.	Inicio de sesión.	RF.001	Permite a cualquier usuario autenticarse en el sistema por medio de identificación y contraseña.
ADMINISTRACIÓN.	Agregar y editar usuario.	RF.002	Permite a los administradores agregar y editar un usuario.
	Agregar auditoría.	RF.003	Permite a los administradores agregar una auditoría.
	Agregar y editar una organización.	RF.004	Permite a los administradores agregar y editar una organización.
	Agregar y editar un área.	RF.005	Permite a los administradores agregar y editar un

			área.
	Agregar y editar una pregunta.	RF.006	Permite a los administradores agregar y editar una pregunta.
	Gestionar una auditoría.	RF.007	Permite a los auditores líderes gestionar una auditoría, lo cual permite administración de documentos, cifrado, generar reportes, ponderar dominios entre otras.
	Cargar documentos	RF.008	Permite a los auditores líderes de cargar documentos necesarios para una auditoría.
	Descargar documentos	RF.009	Permite a los auditores descargar documentos necesarios para una auditoría.
SEGURIDAD.	Cifrar documento.	RF.010	Permite cifrar un documento donde es necesario por la información sensible que se encuentra.
	Asignar rol para auditoría.	RF.011	Permite a los administradores asignar roles a los usuarios que van a realizar una auditoría. Con esto tendrán permisos específicos en el sistema.
REPORTES.	Generación de reportes.	RF.012	Permite a los auditores líderes de una auditoría la generación de

			reportes sobre los resultados de la misma.
INFERENCIA.	Visualización de estadísticas de una auditoría.	RF.013	Permite al auditor líder generar las gráficas de los resultados de una auditoría.

Tabla 4. Lista de requerimientos funcionales.
Fuente: Autores

NOMBRE	IDENTIFICADOR	DESCRIPCIÓN
CONFIDENCIALIDAD.	RNF.001	El sistema permite la protección adecuada de la información sensible que se maneja.
DISPONIBILIDAD.	RNF.002	El sistema permite su uso cuando y donde se necesite.
INTEGRIDAD.	RNF.003	El sistema proporciona la protección adecuada de la información contenida en el mismo.
USABILIDAD.	RNF.004	El sistema es de fácil uso, con pocos pasos el usuario puede crear parámetros para auditoría y realizar el proceso de una de auditoría
APLICATIVO WEB	RNF.005	El sistema debe desarrollarse para un entorno web

Tabla 5. Lista de requerimientos no funcionales.
Fuente: Autores

- Se definió la arquitectura general del sistema, a continuación se presenta la imagen que la representa.

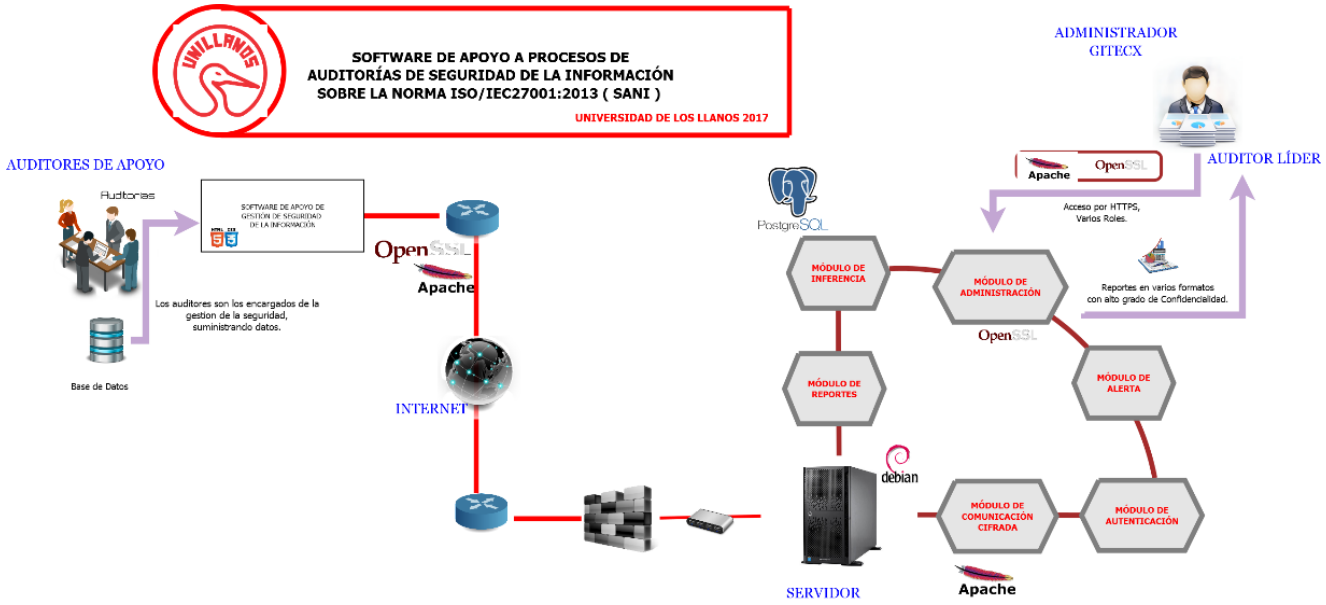


Imagen 1. Arquitectura del sistema
Fuente: Autores

- Aquí se observa los usuarios (administrador, Auditores), los cuales podrán interactuar con el sistema mediante un navegador web.
- También se plasma una serie de módulos que describen las principales funciones del sistema junto con herramientas tecnológicas que utilizara el servidor web para poder soportar el debido funcionamiento del sistema.

7.2. FASE DE ELABORACIÓN

Esta fase constó de dos iteraciones, básicamente se desarrolló el modelado necesario para identificar todo el funcionamiento del sistema.

Actividades.

- Se realizó casos de uso supliendo todos los requerimientos antes definidos, a continuación se muestra el diagrama general.

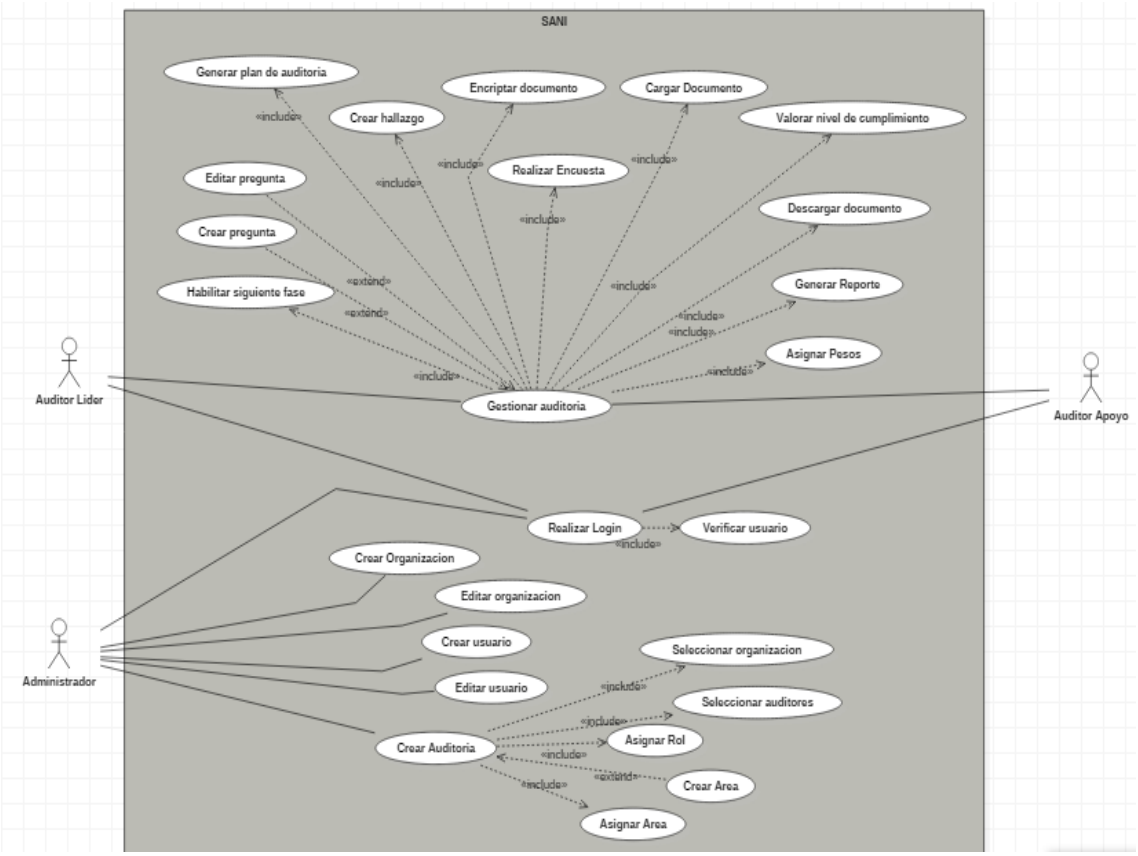


Imagen 2. Diagrama de casos de uso general.
Fuente: Autores

- A continuación se mostrará algunas de las fichas de casos de uso del sistema.

CU001	INICIO DE SESIÓN.	
REQUERIMIENTOS ASOCIADOS	RF.001	
DESCRIPCIÓN	Este caso de uso permite a los usuarios autenticarse ante el sistema, muestra en pantalla un formulario donde se digita el usuario y contraseña.	
PRECONDICIÓN	El usuario debe estar registrado en la base de datos.	
SECUENCIA NORMAL	PASO	ACCIÓN
	1	El usuario ingresa usuario y contraseña.
	2	El sistema SANI verifica que los datos ingresados coincidan con los de la base de datos.
	3	El sistema permite el acceso.
POST-CONDICIÓN	El sistema permite el acceso al usuario.	
SECUENCIA ALTERNATIVA	PASO	ACCIÓN
	2	El sistema SANI verifica que los datos ingresados coincidan con los de la base de datos.
	3	El sistema no permite el acceso al usuario por la no coincidencia de datos ingresados con los de la base de datos.
	4	El usuario ingresa nuevamente sus datos de autenticación.
	5	El sistema SANI verifica que los datos ingresados coincidan con los de la base de datos.
	6	El sistema permite el acceso.

Tabla 6. Caso de uso Iniciar sesión.
Fuente: Autores

CU002	CREAR USUARIO.	
REQUERIMIENTOS ASOCIADOS	RF.002	
DESCRIPCIÓN	El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un administrador solicite crear un usuario.	
PRECONDICIÓN	El administrador debe estar autenticado.	
SECUENCIA NORMAL	PASO	ACCIÓN
	1	El administrador solicita crear un usuario al sistema.
	2	El sistema solicita los datos del usuario que se desea crear.
	3	El administrador proporciona los datos requeridos y solicita al sistema agregar el usuario.
	4	El sistema agrega el usuario al sistema.
POST-CONDICIÓN	El usuario ha sido creado en el sistema.	
SECUENCIA ALTERNATIVA	PASO	ACCIÓN
	4	El sistema notifica que el usuario ya existe en la base de datos.
	5	El sistema vuelve a solicitar datos para el nuevo usuario.

Tabla 7. Caso de uso Crear usuario.
Fuente: Autores

CU006	CREAR AUDITORÍA.	
REQUERIMIENTOS ASOCIADOS	RF.003	
DESCRIPCIÓN	El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un administrador solicite crear una auditoría.	
PRECONDICIÓN	El administrador debe estar autenticado.	
SECUENCIA NORMAL	PASO	ACCIÓN
	1	El administrador solicita crear una

		auditoría al sistema.
	2	El sistema solicita los datos de la auditoría que se desea crear. Los datos son:
	3	El administrador proporciona los datos requeridos y solicita al sistema agregar la auditoría.
	4	El sistema agrega la auditoría al sistema.
POST-CONDICIÓN	La auditoría ha sido creada en el sistema.	
SECUENCIA ALTERNATIVA	PASO	ACCIÓN
		N/A

Tabla 8. Caso de uso Crear auditoria.
Fuente: Autores

CU007	GESTIONAR AUDITORÍA.	
REQUERIMIENTOS ASOCIADOS	RF.007	
DESCRIPCIÓN	El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un auditor líder o auditor de apoyo gestiona una auditoría.	
PRECONDICIÓN	Los auditores deben estar autenticados y encontrarse dentro de un proceso de auditoría en el sistema.	
SECUENCIA NORMAL	PASO	ACCIÓN
	1	Los auditores se encuentran en la primera fase de la auditoría.
	2	Los auditores se encargan de la carga de archivos al sistema (depende del tipo de archivo y si tiene el permiso).
	3	El auditor líder pasa a la siguiente fase de auditoría y se encarga de que por lo menos el 80% de los archivos cargados en la fase 1 sean leídos por todos los auditores en el

		proceso.
	4	Los auditores pueden realizar el llenado de las listas de chequeo y también cargar el archivo de hallazgos para llegar a un acuerdo con todos los auditores del proceso.
	5	El auditor líder genera gráficas de resultados y genera reporte final de auditoría, dando finalización al proceso de auditoría.
POST-CONDICIÓN	Se ha hecho gestión del proceso de auditoría.	
SECUENCIA ALTERNATIVA	PASO	ACCIÓN
		N/A

Tabla 9. Caso de uso Gestionar auditoria
Fuente: Autores

CU011	GENERAR REPORTE.	
REQUERIMIENTOS ASOCIADOS	RF.012	
DESCRIPCIÓN	El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando el auditor líder solicite generar un reporte.	
PRECONDICIÓN	El auditor líder debe estar autenticado y la auditoría donde él participa debe estar en su fase final.	
SECUENCIA NORMAL	PASO	ACCIÓN
	1	El auditor líder ingresa a la última fase de la auditoría.
	2	El auditor solicita generar el reporte final de auditoría.
	3	El sistema toma toda la información que se necesita para generar el documento con el reporte solicitado.
	4	El sistema genera el reporte y está listo para descargar.

POST-CONDICIÓN	El reporte se genera correctamente.	
SECUENCIA ALTERNATIVA	PASO	ACCIÓN
		N/A

Tabla 10. Caso de uso Generar reporte.
Fuente: Autores

- También se define el modelo de entidad relación del sistema, el cual cumple con los requerimientos del sistema. Para el modelo entidad relación se mostrarán las tablas que hacen parte del sistema SANI, se aclara que algunas palabras no tendrán tilde ya que son los nombres de las tablas como están en la base de datos del sistema.

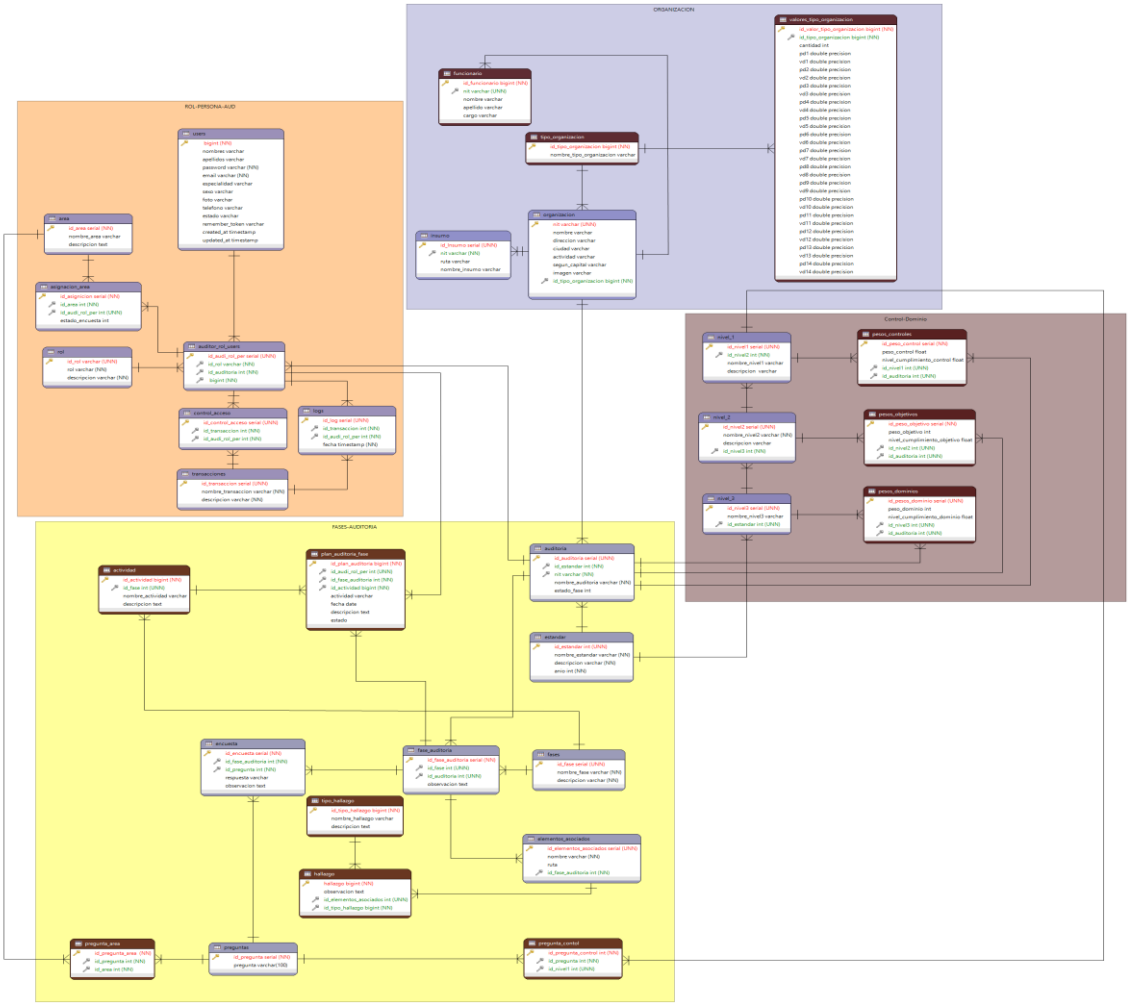


Imagen 3. Diagrama Entidad-Relación general.

Fuente: Autores

- Se describe algunas de las tablas del sistema, a continuación:

NOMBRE ATRIBUTO	TIPO DE DATO	NOT NULL?	DESCRIPCIÓN
nit	Varchar	Si	Identificador consecutivo de la organización.
nombre	Varchar		Nombre de la organización.
direccion	Varchar		Dirección de la organización.
ciudad	Varchar		Ciudad donde se encuentra la organización.
actividad	Varchar		Actividad la cual pertenece la organización.
segun_capital	Varchar		Capital la cual pertenece la organización.
Imagen	Varchar		Imagen de la organización.
Id_tipo_organizacion	Integer	Si	Identificador de tipo de organización.

Tabla 11. organizacion.
Fuente: Autores

NOMBRE LLAVE	TIPO DE LLAVE	DESCRIPCIÓN
nit	Primary key	Llave primaria de la tabla **organizacion.**
id_tipo_organizacion	Foreign key	Llave foránea referenciada a la tabla **tipo_organizacion**.

Tabla 12. Llaves de organizacion.
Fuente: Autores

NOMBRE ATRIBUTO	TIPO DE DATO	NOT NULL?	DESCRIPCIÓN
id_auditoria	Serial	Si	Identificador consecutivo de las auditorías.
id_estandar	Integer	Si	Identificador del estándar.
nit	Varchar	Si	Identificador de la organización.
nombre_auditoria	Varchar	Si	Nombre de la auditoria.

estado_fase	Integer		Estado de fase de la auditoría.

Tabla 13. Auditoria.
Fuente: Autores

NOMBRE LLAVE	TIPO DE LLAVE	DESCRIPCIÓN
id_auditoria	Primary key	Llave primaria de la tabla **auditoria.**
id_estandar	Foreign key	Llave foránea referenciada a la tabla **estandar.**
nit	Foreign key	Llave foránea referenciada a la tabla **organizacion.**

Tabla 14. Llaves de auditoria.
Fuente: Autores

NOMBRE ATRIBUTO	TIPO DE DATO	NOT NULL?	DESCRIPCIÓN
cc	Bigint	Si	Identificacion de la persona.
nombres	Varchar	Si	Nombre de la persona.
apellidos	Varchar	Si	Apellidos de la persona.
sexo	Varchar		Sexo de la persona.
telefono	Bigint		Teléfono de la persona.
email	Varchar	Si	Correo electrónico de la persona.
password	Varchar	Si	Contraseña de la persona.
imagen	Varchar		Imagen de la persona.
especialidad	Varchar		Especialidad de la persona.
remember_token	Varchar		
created_at	Timestamp		
updated_at	Timestamp		

Tabla 15. users.
Fuente: Autores

NOMBRE LLAVE	TIPO DE LLAVE	DESCRIPCIÓN
cc	Primary key	Llave primaria de la tabla **users.**

Tabla 16. Llaves de users.
Fuente: Autores

NOMBRE ATRIBUTO	TIPO DE DATO	NOT NULL?	DESCRIPCIÓN
id_valor_tipo_organizacion	Serial	si	Identificación consecutiva del valor acumulativo de los tipos de organización.
id_tipo_organizacion	Integer	Si	Identificador de tipo de organización.
cantidad	Integer		Cantidad de tipo de organizaciones que realizaron una auditoría.
pd1	Double precision		Valor peso dominio 1 acumulativo por tipo de empresa.
vd1	Double precision		Valor nivel de cumplimiento 1 acumulativo por tipo de empresa.
pd2	Double precision		Valor peso dominio 2 acumulativo por tipo de empresa.
vd2	Double precision		Valor nivel de cumplimiento 2 acumulativo por tipo de empresa.
pd3	Double precision		Valor peso dominio 3 acumulativo por tipo de empresa.
vd3	Double precision		Valor nivel de cumplimiento 3 acumulativo por tipo de empresa.

pd4	Double precision		Valor peso dominio 4 acumulativo por tipo de empresa.
vd4	Double precision		Valor nivel de cumplimiento 4 acumulativo por tipo de empresa.
pd5	Double precision		Valor peso dominio 5 acumulativo por tipo de empresa.
vd5	Double precision		Valor nivel de cumplimiento 5 acumulativo por tipo de empresa.
pd6	Double precision		Valor peso dominio 6 acumulativo por tipo de empresa.
vd6	Double precision		Valor nivel de cumplimiento 6 acumulativo por tipo de empresa.
pd7	Double precision		Valor peso dominio 7 acumulativo por tipo de empresa.
vd7	Double precision		Valor nivel de cumplimiento 7 acumulativo por tipo de empresa.
pd8	Double precision		Valor peso dominio 8 acumulativo por tipo de empresa.
vd8	Double precision		Valor nivel de cumplimiento 8 acumulativo por tipo de empresa.
pd9	Double precision		Valor peso dominio 9 acumulativo por tipo de empresa.
vd9	Double precision		Valor nivel de cumplimiento 9 acumulativo por tipo de empresa.
pd10	Double precision		Valor peso dominio 10

			acumulativo por tipo de empresa.
vd10	Double precision		Valor nivel de cumplimiento 10 acumulativo por tipo de empresa.
pd11	Double precision		Valor peso dominio 11 acumulativo por tipo de empresa.
vd11	Double precision		Valor nivel de cumplimiento 11 acumulativo por tipo de empresa.
pd12	Double precision		Valor peso dominio 12 acumulativo por tipo de empresa.
vd12	Double precision		Valor nivel de cumplimiento 12 acumulativo por tipo de empresa.
pd13	Double precision		Valor peso dominio 13 acumulativo por tipo de empresa.
vd13	Double precision		Valor nivel de cumplimiento 13 acumulativo por tipo de empresa.
pd14	Double precision		Valor peso dominio 14 acumulativo por tipo de empresa.
vd14	Double precision		Valor nivel de cumplimiento 14 acumulativo por tipo de empresa.

Tabla 17.valores_tipo_organizacion.
Fuente: Autores

7.3. FASE DE CONSTRUCCIÓN

Esta fase constó de tres iteraciones, debido a que los módulos desarrollados se integraron y se probaron simultáneamente.

Actividades

Para la construcción de sistema SANI se tuvo en cuenta que por cada iteración se seleccionaran los casos de uso, se refinará su análisis, diseño y se procediera a la implementación y pruebas respectivas. Es importante recalcar que al llegar a la última iteración se obtiene la primera versión de la herramienta web.

- Codificación en el lenguaje de programación JavaScript y Php, se usa el framework Laravel 5.4 y se usa Bootstrap 3.
  A continuación se mostrará los componentes del sistema SANI.

NOMBRE	FUNCIÓN	LOCALIZACIÓN	TAMAÑO	LÍNEAS
ForgotPasswordController.php	Controladores que atienden a las peticiones relacionadas con la parte de administración del sistema.	app/Http/Controller/Auth/	1,04KB	43
LoginController.php		app/Http/Controller/Auth/	2,29KB	93
RegisterController.php		app/Http/Controller/Auth/	2,74KB	102
ResetPasswordController.php		app/Http/Controllers/Auth/	1,29KB	50
AreaController.php		app/Http/Controllers/	1,92KB	97
AuditorController.php		app/Http/Controllers/	3,14KB	124
AuditoriaController.php		app/Http/Controllers/	6,21KB	216
Controller.php		app/Http/Controllers/	361bytes	14
DominiosController.php		app/Http/Controllers/	1,52KB	85
Fase1Controller.php		app/Http/Controllers/	6,26KB	179
Fase2AuxiliarController.php		app/Http/Controllers/	2,32KB	95
Fase2Controller.php		app/Http/Controllers/	2,71KB	103
Fase3AuxiliarController.php		app/Http/Controllers/	2,32KB	94
Fase3Controller.php		app/Http/Controllers/	2,02KB	97
Fase4Controller.php		app/Http/Controllers/	1,58KB	86
Fase5Controller.php		app/Http/Controllers/	1,51KB	86
GeneralidadesController.php		app/Http/Controllers/	1,53KB	86
HomeController.php		app/Http/Controllers/	1,95KB	43
infodominioController.php		app/Http/Controllers/	1,52KB	85
OrganizacionController.php		app/Http/Controllers/	4,29KB	134
pesosController.php		app/Http/Controllers/	1,51KB	85
PreguntasController.php		app/Http/Controllers/	3,58KB	123
area.php	Clases orm correspondientes a las tablas del modelo	app/	267 bytes	17
asignación_area.php		app/	328 bytes	17
Auditor_rol_user.php		app/	310 bytes	17
Auditoria.php		app/	333 bytes	17
Control_Acceso.php		app/	303 bytes	17
Dependencia.php		app/	244 bytes	17
Elementos_Asociados.php		app/	319 bytes	17
Encuestas.php		app/	358 bytes	20
Estandar.php		app/	299 bytes	17
Fase_auditoria.php		app/	294 bytes	17

Fases.php	entidad relación de base de datos.	app/	269 bytes	17
Funcionarios.php		app/	273 bytes	17
Hallazgos.php		app/	105 bytes	10
Información_Riesgo.php		app/	492 bytes	25
Insumo.php		app/	310 bytes	19
Logs.php		app/	290 bytes	17
Nivel_Dos.php		app/	302 bytes	17
Nivel_Tres.php		app/	282 bytes	17
Nivel_Uno.php		app/	302 bytes	17
Organizacion.php		app/	404 bytes	22
Pesos_Controles.php		app/	361 bytes	17
Pesos_Dominios.php		app/	362 bytes	17
Pesos_Objetivos.php		app/	364 bytes	17
pregunta_control.php		app/	304 bytes	17
preguntaArea.php		app/	292 bytes	17
preguntas.php		app/	255 bytes	17
Proceso.php		app/	231 bytes	17
Proceso_Dependencia.php		app/	264 bytes	17
Riesgo.php		app/	358 bytes	20
rol.php		app/	256 bytes	17
tipoInsumo.php		app/	269 bytes	17
Transacciones.php		app/	299 bytes	17
User.php		app/	880 bytes	17
vistas.php		app/	271 bytes	17
2014_10_12_000000_create_users_table.php	Contiene órdenes de creación de las tablas.	database/migrations/	1,01KB	43
2014_10_12_100000_create_password_resets_table.php		database/migrations/	692 bytes	33
2017_04_24_190332_create_organizacions_table.php		database/migrations/	942 bytes	40
2017_04_24_190930_create_estandars_table.php		database/migrations/	752 bytes	35
2017_04_24_191011_create_informacion__riesgos_table.php		database/migrations/	1,13KB	43
2017_04_24_191031_create_procesos_table.php		database/migrations/	778 bytes	35
2017_04_24_191055_create_dependencias_table.php		database/migrations/	802 bytes	35
2017_04_24_191120_create_proceso__dependencias_table.php		database/migrations/	953 bytes	36
2017_04_24_191140_create_fases_table.php		database/migrations/	693 bytes	34
2017_04_24_191150_create_auditorias_table.php		database/migrations/	960 bytes	38
2017_04_24_191158_create_fase__auditorias_table.php		database/migrations/	897 bytes	36
2017_04_24_191222_crea		database/migrations/	899 bytes	36

te_elementos__asociados_table.php				
2017_04_24_191228_create_tipo_insumos_table.php		database/migrations/	686 bytes	33
2017_04_24_191236_create_insumos_table.php		database/migrations/	955 bytes	38
2017_04_24_191250_create_transacciones_table.php		database/migrations/	738 bytes	34
2017_04_24_191302_create_roles_table.php		database/migrations/	697 bytes	34
2017_04_24_191351_create_auditor_rol_users_table.php		database/migrations/	1006 bytes	38
2017_04_24_191411_create_logs_table.php		database/migrations/	941 bytes	37
2017_04_24_191427_create_control__accesos_table.php		database/migrations/	953 bytes	36
2017_04_24_191438_create_riesgos_table.php		database/migrations/	1,10KB	41
2017_04_24_191450_create_funcionarios_table.php		database/migrations/	1,01KB	39
2017_04_24_191652_create_nivel__tres_table.php		database/migrations/	803 bytes	35
2017_04_24_191722_create_nivel__dos_table.php		database/migrations/	839 bytes	36
2017_04_24_191736_create_nivel__unos_table.php		database/migrations/	837 bytes	36
2017_04_24_191936_create_areas_table.php		database/migrations/	681 bytes	34
2017_04_24_192015_create_asignacion__areas_table.php		database/migrations/	908 bytes	36
2017_04_24_192044_create_vistas_table.php		database/migrations/	801 bytes	35
2017_04_24_192101_create_preguntas_table.php		database/migrations/	657 bytes	33
2017_04_24_192117_create_encuestas_table.php		database/migrations/	1,01KB	39
2017_05_19_023448_create_pesos__controles_table.php		database/migrations/	1013 bytes	38
2017_05_19_023535_create_pesos__objetivos_table.php		database/migrations/	1017 bytes	38
2017_05_19_023550_create_pesos__dominios_table.php		database/migrations/	1011 bytes	38
2017_06_06_212903_create_hallazgos_table.php		database/migrations/	953 bytes	38
2017_06_08_224638_create_pregunta__controls_table.php		database/migrations/	924 bytes	36

2017_06_16_012736_create_pregunta_areas_table.php		database/migrations/	898 bytes	36
App.js	Almacena en un arreglo la configuración global de la aplicación.	public/js/	1,14MB	41454
ocultar.js	Script para ocultar vistas.	public/js/	6,14KB	273
ocultarFase1.js	Script para ocultar elementos de la fase 1 de auditoría.	public/js/	1,39KB	62
visualizar.js	Script para visualizar vistas.	public/js/	734bytes	24
Index.php	Lista el número de auditorías donde está participando un auditor.	public/	1,74KB	59
email.blade.php	Despliega las vistas de cada una de las partes del Sistema para el desarrollo de procesos de auditoria en el Sistema.	resources/views/auth/passwords/	1,83KB	47
reset.blade.php		resources/views/auth/passwords/	3,43KB	77
Login.blade.php		resources/views/auth/	2,99KB	69
Register.blade.php		resources/views/auth/	3,44KB	77
home.blade.php		resources/views/vendor/adminlte/	3,87KB	116
area.blade.php		resources/views/vendor/adminlte/Area	3,63KB	104
auditor.blade.php		resources/views/vendor/adminlte/Auditor	3,20KB	100
auditor_crear.blade.php		resources/views/vendor/adminlte/Auditor	4,57KB	109
auditoria.blade.php		resources/views/vendor/adminlte/Auditoria	11,6KB	267
Encuesta_Area.blade.php		resources/views/vendor/adminlte/Auxiliar	105KB	79
Fase2_Auxi.blade.php		resources/views/vendor/adminlte/Auxiliar	5,09KB	108
auditor.blade.php		resources/views/vendor/adminlte/crear	6,40KB	147
auditoria.blade.php		resources/views/vendor/adminlte/crear	7,97KB	200
organizacion.blade.php		resources/views/vendor/adminlte/crear	6,65KB	147
27001dominios.blade.php		resources/views/vendor/adminlte/encuesta	105KB	1703
27001generalidades.blade.php		resources/views/vendor/adminlte/encuesta	58,7KB	935

27001pesos.blade		resources/views/vendor/adminlte/encuesta	153KM	1480
fase1.blade.php		resources/views/vendor/adminlte/fases	11,4KB	209
fase2.blade.php		resources/views/vendor/adminlte/fases	6,76KB	134
fase3.blade.php		resources/views/vendor/adminlte/fases	12KB	112
fase4.blade.php		resources/views/vendor/adminlte/fases	3,16KB	80
fase5.blade.php		resources/views/vendor/adminlte/fases	3,86KB	92
infodominio.blade.php		resources/views/vendor/adminlte/informacion/	141KB	1488
organizacion.blade.php		resources/views/vendor/adminlte/Organizacion/	2,90KB	90
organizacion_agregar.blade.php		resources/views/vendor/adminlte/Organizacion/	4,80KB	109
organizacion_editar.blade.php		resources/views/vendor/adminlte/Organizacion/	4,77KB	109
pregunta_crear.blade.php		resources/views/vendor/adminlte/Pregunta	2,77KB	86
pregunta_editar.blade.php		resources/views/vendor/adminlte/Pregunta	2,80KB	87
pregunta_ver.blade.php		resources/views/vendor/adminlte/Pregunta	2,45KB	88
web.php	Registro de todas las rutas atendidas por el sistema.	routes/	2,12KB	46

Tabla 18.componentes del sistema.

- Se diseñó e integró en el sistema los siguientes componentes de seguridad.

    - **Https:** El protocolo https permite una comunicación segura su implementación se da para los casos en los que el auditor líder de un proceso de auditoría desea mantener cifrados todos los datos que está enviando o descargando del servidor y no permitir que terceros observan la información en la red con programas sniffer como Wireshark (Wireshark · Go Deep. n.d.)
    - **Sesiones:** Las sesiones son un importante componente del sistema ya que permite darle acceso a los usuarios una vez haya pasado por el componente de autenticación, esta sesión se

verifica en cada petición http get o post y las sesiones caducan luego de 1 hora de inactividad previniendo que un tercero se apodere del dispositivo abandonado del usuario, por otra parte, gracias al framework Laravel estas sesiones integran un token autogenerado en cada petición Post, si dicho token no se encuentra activo en la sesión del servidor, el sistema rechaza la petición y arroja un mensaje de error, esto sucede para prevenir ataques CSRF y XSRF (Otwell s.f.).

- Se organizaron los recursos que se usaron en el desarrollo y se realizó una documentación interna.

- Se elaboraron los manuales tanto de usuario como de soporte técnico. Los cuales van como documentos adjuntos a este informe final.

7.4. FASE DE TRANSICIÓN Y ENTREGA FINAL

Estuvo compuesta por tres iteraciones. A continuación, se describe esta fase:

Actividades

- En esta fase se realizaron pruebas de funcionamiento internas y manejo de excepciones dentro del sistema, en las cuales se encontraron una serie de errores lógicos, que fueron ya depurados.

- Además se ejecutó el aplicativo en diferentes navegadores web como Google Chrome, Firefox, Internet Explorer, dando un resultado óptimo.

- Se realizó un video demostrativo de SANI con el fin de abarcar los aspectos más importantes que se deben tener en cuenta para interactuar con el software sin extender la curva de aprendizaje.

Se muestra el caso de estudio del proceso de auditoría de la Facultad de Ciencias Básicas e Ingeniería “FCBI” de la Universidad de los Llanos. Esta facultad tiene 11 dependencias los cuales se tuvieron en cuenta 4 para el caso de prueba de la auditoría.

Dependencia	Activos de Información	Normatividad	Riesgos.
Decanatura.	• Credenciales de acceso institucionales.	• Acuerdo Sup. 012 e 2009.	• Suplantación. • Desprestigio institucional.

	• Correspondencia. • Hojas de vida. • Convenios.	• Acuerdo Sup. 004 de 2009.	• Lucro cesante.
Secretaria Académica.	• Actas de consejo. • Credenciales de acceso. • Resultados evaluación docente.	• Acuerdo Sup. 012 e 2009. • Acuerdo Sup. 004 de 2009.	• Suplantación. • Desprestigio institucional. • Lucro cesante.
Departamento de Matemáticas y Física.	• Credenciales de acceso a sistema SARA. • Hojas de vida docentes.	• Acuerdo Sup. 012 e 2009. • Acuerdo Sup. 004 de 2009.	• Suplantación. • Fraude. • Denegación de servicio.
Proyección social	• Bitácoras de los convenios. • Información de egresados. • Credenciales.	• Acuerdo Sup. 021 de 2002. • Acuerdo Sup. 004 de 2009. • Acuerdo Sup. 012 de 2009.	• Hurto. • Fraude. • Denegación de servicio. • Suplantación.

Tabla 19: Dependencias de la FCBI, en el caso de prueba.

Estas dependencias fueron auditadas en el área de seguridad, bases de datos y sistemas operativos; para la valorización se tuvo en cuenta el Anexo A normativo de la ISO/IEC 27701:2013, contando con una lista de 114 controles que conforman 14 dominios, donde se le dio una prioridad de 18% a la criptografía, un 15% a la seguridad física y ambiental y 10% a la seguridad de las operaciones.
Para este proceso de auditoría se crearon usuarios para tres estudiantes pertenecientes al grupo de investigación y al director de Gitecx experto en seguridad de la información, esto por medio de la interfaz de SANI.
El sistema SANI fue equipado con un sistema de autenticación segura y cifrada con protocolos de seguridad para el envío de información.

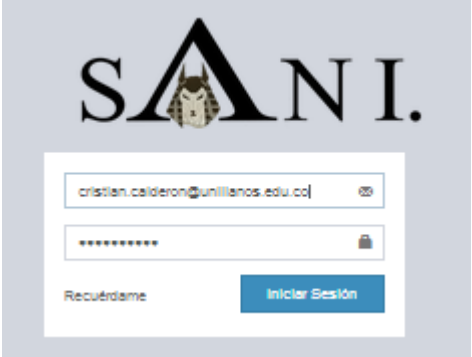


Imagen 4: Módulo de autenticación SANI.

El sistema se instala en 3 equipos de cómputo del Laboratorio del grupo de investigación Gitecx, en los cuales se realizó el proceso de auditoría para las dependencias de la FCBI.
El auditor líder una vez al crear la auditoría asigna a los auxiliares que participaran en la auditoria dando inicio al plan de auditoría.

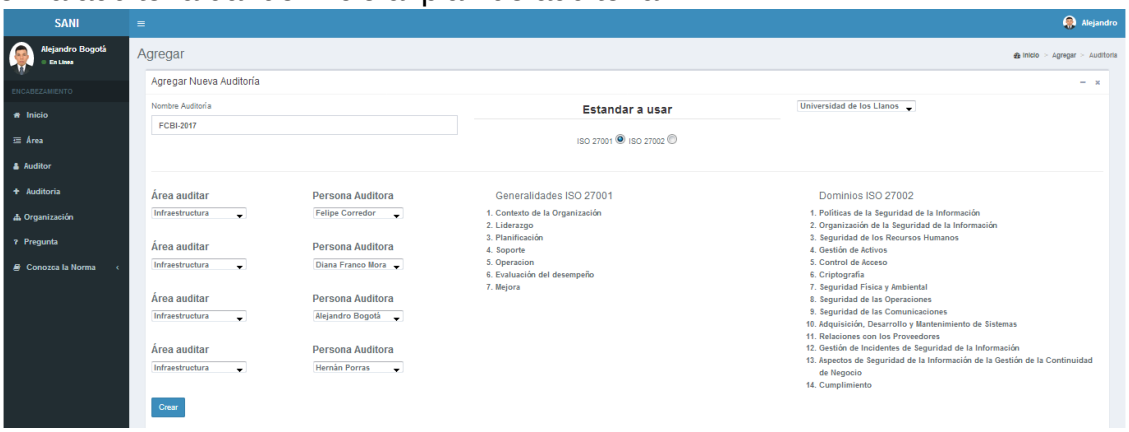


Imagen 5: Creación de Auditoría.

Se verifico la funcionalidad del sistema SANI, al comparar cada resultado de los valores de los niveles de cumplimiento de la auditoría, y se hizo un breve análisis a los informes generados por el sistema desde su interfaz.

Imagen 6: Acceso y progreso de Auditoría.

Para el sistema SANI se realizó una interfaz amigable a los usuarios para que ellos puedan realizar completamente el total del proceso de auditoría que se les asigne. También, se incorporan mecanismos de seguridad ayudando a aminorar riesgos de suplantación o fraude sobre información de la organización en el transcurso de la auditoría, igual asesorándose de la integridad, disponibilidad y confiabilidad de la información.

SANI es un sistema que plasma con los necesarios y más distinguidos rasgos en gestión de la seguridad, enfocándose en cifrado de credenciales y datos sensibles, facilidad de uso, análisis de resultados y reportes con detalles gráficos y estadísticos.

8. RESULTADOS

- SANI versión 1.0 accesible desde la web para la comunidad universitaria y organizaciones.

Imagen 8. VISTA PRINCIPAL.

- Componentes de seguridad: la aplicación integra diferentes componentes de seguridad como: autenticación, https y sesiones; cada uno de estos detallado en la fase de construcción.

- Documentación técnica y de usuario pertinente; se encuentra alojada en la carpeta “manuales”.

- Documentos que hacen parte del sistema como lo son: acta de asistencia, acuerdo de hallazgos, formatos de confidencialidad y de reportes.

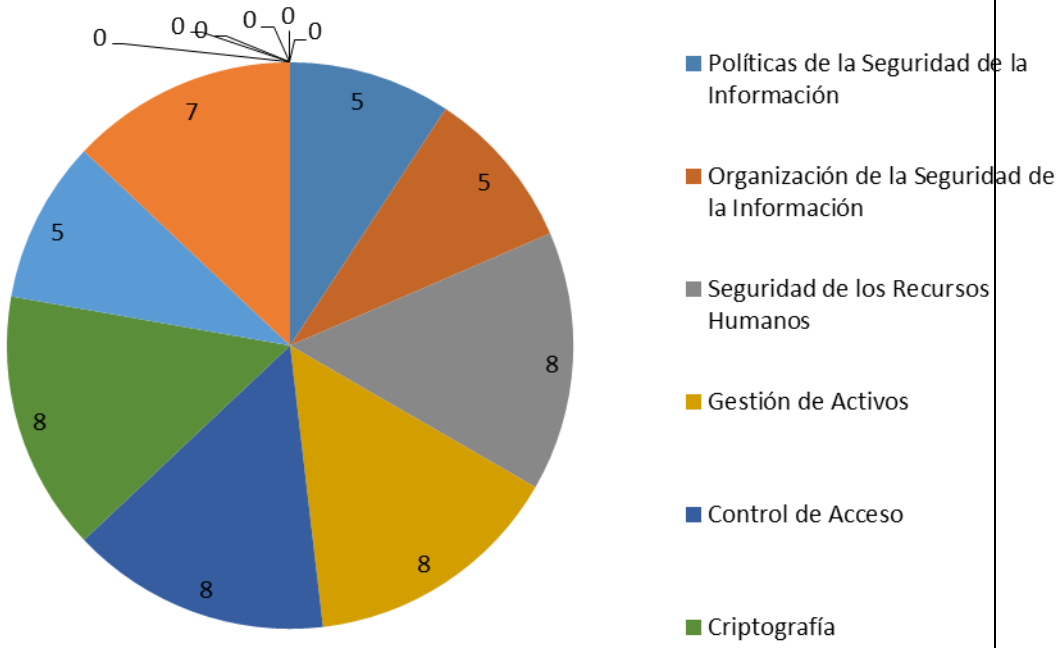
Universidad de los Llanos
Facultad de Ciencias Básicas e Ingenierías
Programa de Ingeniería de Sistemas
Grupo de Investigación en tecnologías abiertas - GITECX

Introducción

La ejecución de la auditoría se realizó en la Universidad de los Llanos, el cual busca evaluar el proceso y eficiencia en el manejo de la información de esta organización, en la siguiente tabla se muestra la información de la organización, lo cual se realizó por medio de la norma ISO/IEC 27001 y 27002 del 2013.

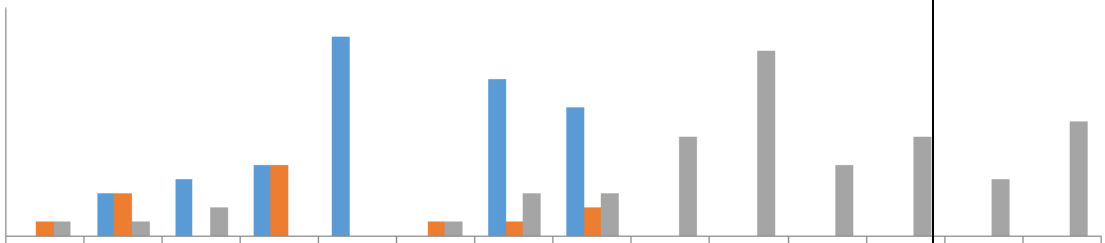
Nit	**892000757-3**
Nombre	Universidad de los Llanos
Dirección	Km. 12 Vía Puerto López
Ciudad	Villavicencio
Sector	Educación

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.



El valor de los dominios se asignó teniendo en cuenta el contenido del control y el activo de información.

El conjunto de controles se le asignó un puntaje de la valoración, el cual indica el nivel de cumplimiento siendo alto (mayores de 75 puntos), medio (entre 30 y 74 puntos) y bajo (menos de 30 puntos). Como se evidencia en la siguiente grafica de puntaje por control vs. Dominios.



	Políticas de la Seguridad de la Información	Organización de la Seguridad de la Información	Seguridad de los Recursos Humanos	Gestión de Activos	Control de Acceso	Criptografía	Seguridad Física y Ambiental	Seguridad de las Operaciones	Seguridad de las Comunicaciones	Adquisición, Desarrollo y Mantenimiento de Sistemas	Relaciones con los Proveedores	Gestión de Incidentes de Seguridad de la Información	Aspectos de Seguridad de la Información de la Gestión de...	Cumplimiento
Series1	0	3	4	5	14	0	11	9	0	0	0	0	0	0
Series2	1	3	0	5	0	1	1	2	0	0	0	0	0	0
Series3	1	1	2	0	0	1	3	3	7	13	5	7	4	8

A continuación se muestra la gráfica de comparación del nivel de cumplimiento ideal vs el actual de la organización referente a los dominios de la norma.

Imagen 9. REPORTE EJECUTIVO

- Artículo que presenta el desarrollo tecnológico, el cual lo podrá encontrar en la carpeta artículo.

9. CONCLUSIONES

- La herramienta para auditoría, constituye un enfoque moderno que persigue obtener resultados completos e inmediatos en la evaluación efectuada a las diferentes áreas de una empresa, permitiendo de manera oportuna y completa, presentar los resultados de alta calidad para la realización de informes y toma de decisiones.
- La herramienta será explotada y generará un impacto regional, ya que por parte del curso de teleinformática III será usada por los estudiantes para entornos reales en la región, realizando auditorías propuestas a las organizaciones y mostrando resultados, y así generar un histórico de los puntajes de procesos de auditorías según el tipo de organización, para auditorias futuras.

- El proceso de auditoria con la herramienta será más simple y asequible para realizar procesos de auditoría a cualquier tipo de organización, pues el sistema estará disponible para cuando y donde sea necesario incluyendo seguridad como prioridad para la organización.

10. REFERENCIAS

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

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

[3] “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.

[4] 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.

[5] F. A. Corredor, “Asistente metodológico basado en inferencia y orientado a la web; para la implementación de Auditorias de seguridad de la información sobre las norma ISO/IEC 27001.,” pp. 1–19, 2015.

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

[7] “The ISO Survey,” *certificaciones ISO 27001 Mundial*. [Online]. Available: https://www.iso.org/the-iso-survey.html. [Accessed: 28-Jul-2017].

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

[9] Trend Micro and Oea, “Reporte de Seguridad Cibernética e Infraestructura

Crítica de las Américas," 2015.

[10] Symantec Corporation, "Internet Security Threat Report," vol. 21, no. April, p. 81, 2016.

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

[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] "Auditoria de la información y gestión del conocimiento." [Online]. Available: http://www.ainia.es/insights/auditoria-de-la-informacion-y-gestion-del-conocimiento/. [Accessed: 04-Aug-2017].

[14] L. F. Momphotes Parra and J. A. Alzate López, "Prototipo Para La Auditoria Sistema De Gestion Seguridad De La Informacion (SGSI)," p. 79, 2014.

[15] V. M. BECERRA, "Aprovechamiento de tecnologías de información e institucionalización de la seguridad informática en empresas del sector financiero en Colombia," 2002.

[16] "Su empresa tiene los controles adecuados sobre los riesgos de ciberseguridad? - Auditoría & Co." [Online]. Available: http://auditoria-auditores.com/articulos/articulo-auditoria-su-empresa-tiene-los-controles-adecuados-sobre-los-riesgos-de-ciberseguridad-/. [Accessed: 04-Aug-2017].

[17] F. R. Cardenas, "Administración del riesgo cibernetico un enfoque desde la alta gerencia empresarial en Colombia," 2017.

[18] "El análisis de los riesgos de ciberseguridad dentro de la estrategia general del negocio - El blog de UHY FAY & CO. Madrid." [Online]. Available: http://www.elblogdetusasesores-consultores.com/ciberseguridad-y-accesibilidad-de-la-informacion/analisis-los-riesgos-ciberseguridad/. [Accessed: 04-Aug-2017].

[19] J. O. González, "Sistema de Gestión de Seguridad de la Información-SGSI bajo la norma ISO/IEC 27001: 2013 para la empresa 'en Línea Financiera' de la ciudad de Cali–Colombia.," 2017.