Panorama de riesgo tecnológico y la medición del mismo, para la función informática que apoya el proceso de la administración de justicia en la rama judicial de Santander

AUTOR:

JUAN SEBASTIAN CHANAGÁ VARGAS

PROYECTO DE GRADO

DIRECTOR
ING.DANIEL ARENAS SELEEY

ASESOR EXTERNO
JOSE ALFREDO SARMIENTO RODRIGUEZ

UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA UNAB

FACULTAD DE INGENIERÍA

TABLA DE CONTENIDO

PLANTEAMIENTO DEL PROBLEMA Y JUSTIFICACIÓN

Se requiere realizar auditoría de sistemas a la rama judicial del departamento de Santander mediante la elaboración de un panorama de riesgo tecnológico y la clasificación del mismo, puesto que actualmente no existe un informe interno ni externo sobre la función informática. Para ello se requiere investigar en primera instancia qué metodologías existen para el levantamiento y clasificación de riesgo tecnológico y posteriormente aplicarlas en la rama judicial de Santander, para finalmente elaborar un informe de auditoría.

La auditoría de los Sistemas de Información está definida como aquella auditoría

que contempla el estudio, revisión y valoración de todos los elementos (o parte de ellos) de los sistemas automáticos de procesamiento de la información, incluyendo operaciones no automáticas relacionadas con ellos y su interfaz correspondiente, es por ello que se requiere realizar el panorama de riesgo tecnológico y la medición del mismo teniendo en cuenta el estado del arte, evaluación e implementación de las metodologías estándares internacionales, para la función informática que apoya el proceso de la administración de justicia en la rama judicial de Santander. Al realizar este proyecto de auditoría se podrá tener un control interno de la función informática en la rama judicial de Santander.

Pregunta de investigación

¿Cuál es la importancia de la realización de un levantamiento de panorama de riesgo tecnológico en la Rama Judicial de Santander?

Hipótesis de investigación

La realización de una auditoría de sistemas en donde se realice un panorama de riesgo tecnológico permitirá a la rama judicial de Santander tener un control interno de la función informática.

OBJETIVOS PARA REALIZAR EL LEVANTAMIENTO DEL PANORAMA DE RIESGO TECNOLÓGICO

Para realizar el levantamiento del panorama de riesgo tecnológico se requiere de cumplir con una serie de objetivos que llevarán consigo la elaboración de una serie de actividades.

OBJETIVO GENERAL

Realizar el panorama de riesgo tecnológico y la medición del mismo, aplicando una metodología de análisis de riesgos adecuada para la función informática que apoya el proceso de la administración de justicia en la rama judicial de Santander.

Para poder cumplir con el objetivo general se deben tener en cuenta los siguientes objetivos específicos:

OBJETIVOS ESPECÍFICOS

- Realizar un estado del arte de las metodologías para el levantamiento y clasificación del riesgo.
- Efectuar un diagnóstico en la Rama Judicial de Santander, para identificar cuál de las metodologías encontradas es la más adecuada.
- Realizar el panorama de riesgo tecnológico en la Rama Judicial de Santander aplicando la metodología seleccionada en el objetivo 2

MARCO TEÓRICO O ESTADO DEL ARTE

El presente proyecto tiene como objetivo realizar el panorama de riesgo tecnológico y la medición del mismo, aplicando una metodología de análisis de riesgos adecuada para la función informática que apoya el proceso de la administración de justicia en la rama judicial de Santander. Razón por la cual en primera instancia se debe tener conocimiento de la auditoría de sistemas y todo lo que está relacionado con ella como el panorama de riesgo tecnológico, además de entender cómo funciona la Rama Judicial.

Auditoría de sistemas

“La auditoría de los Sistemas de Información está definida como aquella auditoría que contempla el estudio, revisión y valoración de todos los elementos (o parte de ellos) de los sistemas automáticos de procesamiento de la información, incluyendo operaciones no automáticas relacionadas con ellos y su interfaz correspondiente. Existe un requerimiento de promulgación y desarrollo de Normas Generales para este tipo de auditoría ya que tiene una naturaleza especializada y requiere de habilidades específicas por parte del auditor”. (GRANT THORNTON COLOMBIA,2017).

Una adecuada planificación de la auditoría informática debe seguir una serie de gestiones previas permitiendo dimensionar el volumen y particularidades del área dentro de la institución a auditar, los tipos de sistemas, disposición y equipos. Estaciones de trabajo, redes de comunicaciones o servidores son revisados exhaustivamente para posteriormente puntualizar las fragilidades presentes en dichos elementos permitiendo saber la realidad de sus activos de información en cuanto a resguardo, control y medidas de seguridad.

Objetivos de la auditoría de sistemas

Control de la Función Informática, analizar la eficiencia de los sistemas informáticos, verificar el cumplimiento de la normativa en este ámbito, revisar la eficaz gestión de los recursos informáticos, comprobar la seguridad de la información.

Etapas de la auditoría

Etapa de diagnóstico
Conocimiento de negocio (a que se dedica la rama judicial de Santander y como está dividida).
Conocimiento de la función informática: ¿Qué hay? Y ¿qué está fallando? (Hardware, software, bases de datos, mantenimiento, administración, sistemas informáticos, seguridad).

Etapa de justificación
Se elabora un panorama de riesgos.
Medición de riesgos (empleando la metodología DELPHY).
Se realiza la matriz de riesgos. (estableciendo un porcentaje tanto a riesgos como a causas).

Etapa de adecuación
Se realiza un plan de auditoría.

Etapa de formalización
Se da el visto bueno a la auditoría.

Etapa de desarrollo
Se hace un levantamiento de evidencias y un informe de auditoría.

Etapa de implantación
Se realiza un plan de implantación lo cual facilitará posteriores auditorías.

Elementos en los que se enfoca la auditoría

Uso no autorizado, daño o destrucción, Robo, Integridad de la información, efectividad y eficiencia.

Tipos de auditorías

Centro de cómputo, redes, bases de datos, aplicaciones en producción, desarrollo de software, administración y organización al área de informática, aplicativos de ofimática y afines, sistemas operativos, seguridad informática.

Perfil del auditor

Desarrollo informático, gestión de proyectos y ciclo de vida de un proyecto de desarrollo, análisis de riesgos en un entorno informático, telecomunicaciones, gestión bases de datos, gestión de la seguridad de los sistemas a través de planes de contingencia de la información.

G. Colombia, "Todo lo que necesitas saber sobre la Auditoría de sistemas de información. - Grant Thornton Colombia", Grant Thornton Colombia, 2017. [Online]. Available: http://blog.grantthornton.com.co/actualidad/todo-lo-que-necesitas-saber-sobre-la-auditoria-de-sistemas-de-informacion/. [Accessed: 25- Oct- 2018].

Para realizar el panorama de riesgo primero debemos conocer que es la rama judicial y cual es su función.

Definición de la rama judicial

“La Rama judicial es la encargada de administrar la justicia en el Estado colombiano. Está compuesta por distintos órganos articulados del poder público destinado a dirimir conflictos conforme al derecho colombiano”.
Ramajudicial.gov.co. [Online]. Available: https://www.ramajudicial.gov.co/. [Accessed: 26- Aug- 2018].

Un factor elemental a la hora de realizar la auditoría de sistemas es el de identificar el riesgo tecnológico existente que se puede presentar en el hardware, software, sistemas de información y bases de datos. Para ello vamos a definirlo:

Después de definir la auditoría de sistemas, otro aspecto importante a tener en cuenta es que metodología para el análisis del riesgo es la adecuada para realizar un correcto panorama de riesgo tecnológico en la Rama Judicial de Santander, para eso se deben estudiar las metodologías estándares internacionales.
Entre las más reconocidas tenemos COBIT, ITIL E ISO.

Metodologías para levantamiento de riesgo

COBIT

“COBIT fue creado para ayudar a las organizaciones a obtener el valor óptimo de TI manteniendo un balance entre la realización de beneficios, la utilización de recursos y los niveles de riesgo asumidos. COBIT 5 posibilita que TI sea gobernada y gestionada en forma holística para toda la organización, tomando en consideración el negocio y áreas funcionales de punta a punta, así como los interesados internos y externos. COBIT 5 se puede aplicar a organizaciones de todos los tamaños, tanto en el sector privado, público o entidades sin fines de lucro”(Soto, 2016) .

Principios de COBIT

Satisfacer las necesidades del accionista
Considerar la empresa de punta a punta
Aplicar un único modelo de referencia integrado
Posibilitar un enfoque holístico
Separar gobierno de la gestión.

Habilitadores de COBIT

Principios, políticas y modelos de referencia
Procesos
Estructuras organizacionales
Cultura, ética y comportamiento
Información
Servicios, infraestructura y aplicaciones
Gente, habilidades y competencias.

COBIT 4.1

"COBIT se enfoca en qué se requiere para lograr una administración y un control adecuado de TI, y se posiciona en un nivel alto. COBIT ha sido alineado y armonizado con otros estándares y mejores prácticas más detalladas de TI. COBIT actúa como un integrador de todos estos materiales guía, resumiendo los objetivos clave bajo un mismo marco de trabajo integral que también se alinea con los requerimientos de gobierno y de negocios". (Soto,2016)

Los beneficios de implementar COBIT como marco de referencia de gobierno sobre TI incluyen:
• Mejor alineación, con base en su enfoque de negocios
• Una visión, entendible para la gerencia, de lo que hace TI
• Propiedad y responsabilidades claras, con base en su orientación a procesos
• Aceptación general de terceros y reguladores
• Entendimiento compartido entre todos los Interesados, con base en un lenguaje común
• Cumplimiento de los requerimientos COSO para el ambiente de control de TI.

D. Soto, "¿Qué es Cobit y para qué sirve? - Principios de Cobit 5", Nextech Education Center, 2016. [Online]. Available: https://nextech.pe/que-es-cobit-y-para-que-sirve/. [Accessed: 27- Aug- 2018].

ITIL

“Information Technology Infrastructure Library (ITIL), es una metodología que se basa en la calidad de servicio y el desarrollo eficaz y eficiente de los procesos que cubren las actividades más importantes de las organizaciones en sus Sistemas de Información y Tecnologías de Información”. (Coremain,2018)

En la actualidad, esta ‘biblioteca’, aceptada a nivel mundial para la administración de servicios TI, cuenta con cinco libros:

Estrategia del servicio
Diseño del servicio
Transición del servicio
Operación del servicio
Mejora constante del servicio

“Con la gestión de servicios ITIL la empresa se vuelve más competitiva al reaccionar eficazmente a las prioridades de su nicho de mercado. Conseguimos, de esta manera, más fortaleza para competir y minimizamos riesgos y aumentamos la productividad y la eficiencia gracias a que con esta amplia base de datos digitalizada se segmentan mejor las prioridades y se trabaja con más perspectiva”. (Coremain,2018)

Coremain, 2018. [Online]. Available: http://www.coremain.com/metodologia-itil/. [Accessed: 25- Aug- 2018].

ISO 19011 2018

Según Lopez Patiño La nueva guía de auditoría para auditar los sistemas de gestión de las organizaciones presenta los siguientes cambios:

Adición de un nuevo principio de auditoría – “enfoque basado en el riesgo”-, con consejos sobre riesgos de auditoría y oportunidades, e información sobre la forma de aplicarlo.

Expansión de las directrices para la gestión de un programa de auditoría, incluidos sus riesgos.

Expansión de las directrices para la conducción de una auditoría, en particular en la sección de planificación.

Expansión de los requisitos generales de competencia para auditores.
Ajuste de la terminología para reflejar el proceso y no el objeto.

Eliminación del anexo que contiene requisitos de competencia para la auditoría de disciplinas de sistemas de gestión específicos. Debido al amplio número de normas individuales sobre sistemas de gestión, no resulta práctico incluir requisitos de competencias para todas las disciplinas.

J. Lopez Patiño, "ISO 19011:2018, la nueva guía de auditoría para auditar los sistemas de gestión de las organizaciones. | Visión Industrial", ISO 19011:2018, la nueva guía de auditoría para auditar los sistemas de gestión de las organizaciones. | Visión Industrial, 2018. [Online]. Available: http://www.visionindustrial.com.mx/industria/calidad/iso-190112018-la-nueva-guia-de-auditoria-para-auditar-los-sistemas-de-gestion-de-las-organizaciones. [Accessed: 18- Oct- 2018].

METODOLOGÍA

En esta tabla se definirán las actividades a realizar para cada objetivo especifico y a su vez los resultados para cada objetivo.

Tabla 1: Actividades a realizar y su relación con los objetivos del proyecto

OBJETIVO GENERAL	OBJETIVOS ESPECIFICOS	ACTIVIDADES	RESULTADOS

Realizar el panorama de riesgo tecnológico y la medición del mismo, aplicando una metodología de análisis de riesgos adecuada para la función informática que apoya el proceso de la administración de justicia en la rama judicial de Santander.	Realizar un estado del arte de las metodologías para el levantamiento y clasificación del riesgo.	● Crear una bibliografía acerca de las metodologías empleadas para el levantamiento y clasificación del riesgo. ● Crear un informe en donde se resuma cada metodología relacionada.	● Documento con el estado del arte de las metodologías para el levantamiento y clasificación del riesgo.
	Efectuar un diagnóstico en la Rama Judicial de Santander, para identificar cuál de las metodologías encontradas es la más adecuada.	● Realizar una investigación sobre la función informática de la rama judicial de Santander. ● Realizar una etapa de diagnóstico, en la que se pueda conocer la función informática (¿Qué hay?, ¿qué está fallando?	● Diagnóstico en la Rama Judicial de Santander, identificando cuál de las metodologías encontradas es la más adecuada.
	Realizar el panorama de riesgo tecnológico en la Rama Judicial de Santander aplicando la metodología seleccionada en el objetivo 2	● Elaborar un panorama de riesgos. ● Realizar una adecuada medición de riesgos empleando la metodología DELPHY.	● Documento en donde se presente el panorama de riesgo tecnológico en la Rama Judicial de Santander aplicando la metodología seleccionada en el objetivo 2.

RESULTADOS OBTENIDOS

En esta tabla se puede observar una comparación entre las metodologías para realizar un panorama de riesgo tecnológico y de esa manera seleccionar la más adecuada para la Rama judicial de Santander

1) METODOLOGÍAS PARA EL LEVANTAMIENTO Y CLASIFICACIÓN DEL RIESGO

Metodología	Definición	Característica	Usos/Aplicación
COBIT	El COBIT es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso.	Orientado al negocio · Alineado con estándares y regulaciones "de facto" · Basado en una revisión crítica y analítica de las tareas y actividades en TI · Alineado con estándares de control y auditoría (COSO, IFAC, IIA, ISACA, AICPA	COBIT se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes

ITIL	Marco de referencia que describe un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI, con un enfoque de administración de procesos.	• Estrategia de servicios. • Diseño de servicios • Transición de servicios. • Operación de servicios. • Mejora continua de servicios.	Se aplica a cualquier empresa que tenga formalizada la gestión de TI

ISO	Directrices para los Sistemas de Gestión de Auditoría -, referencia para todos los procesos de auditoría interna y externa de los distintos sistemas de gestión basados en estándares de ISO, como ISO 9001, ISO 14001, ISO 27001, ISO 45001	• Adición de un nuevo principio de auditoría – "enfoque basado en el riesgo"-, con consejos sobre riesgos de auditoría y oportunidades, e información sobre la forma de aplicarlo. • Expansión de las directrices para la gestión de un programa de auditoría, incluidos sus riesgos. • Expansión de las directrices para la conducción de una auditoría, en particular en la sección de planificación.	La norma es aplicable a todas las organizaciones que necesitan planear y llevar a cabo auditorías internas o externas de sistemas de gestión o administrar un programa de auditoría, ya sea para mantenimiento o para certificación. En este último caso, también se deben considerar los requisitos de ISO IEC 17021.

Después de realizada la comparación se escoge la metodología COBIT para realizar el panorama de riesgo tecnológico en la rama judicial de Santander debido a que es un estándar mundial en este tipo de auditoría y se tiene un conocimiento de la misma, descartando totalmente Itil puesto que no se cuenta en principio con una formalización de la gestión TI.

2) ETAPA DE DIAGNÓSTICO

En esta etapa procedemos a identificar la función informática existente en la Rama judicial de Santander.

De la función informática debemos tener en cuenta: Sistemas de información, hardware, software, redes, mantenimiento, investigación, tecnología y usuarios.

En la rama judicial de Santander se emplean los siguientes sistemas de información:

Justicia XXI
Reparto
Justicia XXI WEB
TYBA
PORTAL DE DEPÓSITOS JUDICIALES BANAGRARIO
SIIF
KACTUS
SAPHIRO
SICOF

En cuanto a Software se cuenta con:

SQL server 2003, 2005 y 2008
Windows 8.1
Office 365 sin paquete completo
Cicero
VLC

Nero
Aula City
Cipos 472.

Auditoría realizada al hardware en la Rama Judicial de Santander

Equipos de computo

No.	Ciudades	Seccional	Equipos de Cómputo en la Rama Judicial fuera de garantía	Equipos de Continuidad
79	BARBOSA - SANTANDER	BUCARAMANGA	13	1
80	BARRANCABERMEJA	BUCARAMANGA	108	1
81	BUCARAMANGA	BUCARAMANGA	1483	10
82	CABRERA	BUCARAMANGA	1	1
83	CALIFORNIA	BUCARAMANGA	2	1
84	CAPITANEJO	BUCARAMANGA	3	1
85	CARCASI	BUCARAMANGA	3	1
86	CHARALÁ	BUCARAMANGA	13	1
87	CIMITARRA	BUCARAMANGA	10	1
88	FLORIDABLANCA	BUCARAMANGA	38	1
89	GIRÓN	BUCARAMANGA	24	1
90	LEBRIJA	BUCARAMANGA	5	1
91	MÁLAGA	BUCARAMANGA	17	1
92	OIBA	BUCARAMANGA	6	1
93	PIEDECUESTA	BUCARAMANGA	22	1
94	PUENTE NACIONAL	BUCARAMANGA	16	1
95	SABANA DE TORRES	BUCARAMANGA	4	1
96	SAN GIL	BUCARAMANGA	129	1
97	SAN VICENTE DE CHUCURÍ	BUCARAMANGA	10	1
98	SOCORRO	BUCARAMANGA	55	1
99	VÉLEZ	BUCARAMANGA	37	1

Tabla en donde se muestran los dispositivos de cómputo disponibles en la Rama judicial de Santander.

Impresoras

No.	Ciudades	Seccional	Total Impresoras	Impresoras en Garantia	Impresoras Fuera de Garantia	Impresoras en comodato
76	BARBOSA - SANTANDER	BUCARAMANGA	11		11	0
77	BARRANCABERMEJA	BUCARAMANGA	70		68	2
78	BUCARAMANGA	BUCARAMANGA	609		517	92
79	CABRERA	BUCARAMANGA	2		2	0
80	CALIFORNIA	BUCARAMANGA	2		2	0
81	CAPITANEJO	BUCARAMANGA	4		4	0
82	CARCASI	BUCARAMANGA	2		2	0
83	CHARALÁ	BUCARAMANGA	9		9	0
84	CIMITARRA	BUCARAMANGA	10		9	1
85	FLORIDABLANCA	BUCARAMANGA	30		30	0
86	GIRÓN	BUCARAMANGA	17		16	1
87	LEBRIJA	BUCARAMANGA	3		0	3
88	MÁLAGA	BUCARAMANGA	11		11	0
89	OIBA	BUCARAMANGA	5		5	0
90	PIEDECUESTA	BUCARAMANGA	17		16	1
91	PUENTE NACIONAL	BUCARAMANGA	12		12	0
92	SABANA DE TORRES	BUCARAMANGA	4		4	0
93	SAN GIL	BUCARAMANGA	100		100	0
94	SAN VICENTE DE CHUCURÍ	BUCARAMANGA	9		9	0
95	SOCORRO	BUCARAMANGA	40		40	0
96	VÉLEZ	BUCARAMANGA	19		17	2

Tabla con la disponibilidad de impresoras en la Rama judicial de Santander

Servidores

CIUDADES	TOTAL SERVIDORES	SERVIDORES FUERA DE GARANTÍA	SERVIDORES EN GARANTIA
BUCARAMANGA	15	12	3
SAN GIL	1	1	

Tabla con información sobre los servidores disponibles en la Rama judicial de Santander.

Switches

Seccionales	Equipos Activos	Sin Garantía
BUCARAMANGA	65	57

Tabla con información sobre los Switches disponibles en la Rama judicial de Santander.

UPS

CIUDAD	UPS sin garantía	UPS con garantía	TOTAL UPS
BUCARAMANGA	33	0	33

Tabla con información sobre las UPS disponibles en la Rama judicial de Santander.

Portátiles

No.	TIPO EQUIPO	SECCIONAL	CIUDAD	MARCA	MODELO	CANTIDAD
23	PORTATIL	BUCARAMANGA	BARRANCABERMEJA	PC SMART	PC SMART GOB70M	1
24	PORTATIL	BUCARAMAN	BUCARAMAN	DELL	DELL	3

		GA	GA		LATITUDE 2120	
25	PORTATIL	BUCARAMANGA	BUCARAMANGA	PC SMART	PC SMART GOB70M	1

Tabla con información sobre los portátiles disponibles en la Rama judicial de Santander.

Redes y comunicaciones

Al año 2019 existen 17 puntos WAN, de los cuales uno de los puntos es el Palacio de Justicia.

Existen 5 LAN tendidas en Florida, Girón, El Frente, Almacén y la alcaldía (administrativa).

Existen 53 puntos más de WAN en diferentes municipios que cuentan con restricción de políticas de uso de red y de internet.

Mantenimiento

La Rama Judicial de Santander cuenta con una mesa de ayuda contratada, en donde cada trabajador se especializa en un determinado problema.

Existe mesa de ayuda en Bucaramanga, San gil, Barrancabermeja y Socorro.

Investigación y tecnología

Se cuenta con proyectos de:

Seguridad
Digitalización de archivos
WAN
Software administrativo

Usuarios

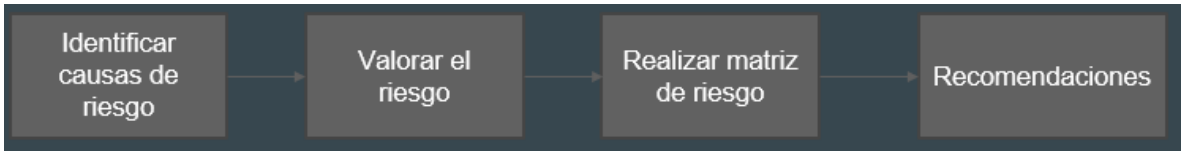
Existe una cantidad de 1800 usuarios, 1000 desde los últimos 3 años y 800 desde hace aproximadamente 10 años.

Diagnóstico de metodología

Después de identificada la función informática de la rama judicial de Santander, y sus características, se procede a escoger la metodología adecuada para el levantamiento del panorama de riesgo tecnológico.

RAMA JUDICIAL	Metodología		
	COBIT	ITIL	ISO
Conocimiento de la metodología	Si	Si	No
Auditoría para gestión y control de cualquier empresa	Si	No	Si
Orientado al negocio especificamente	Si	No	No
Orientado a todos los sectores de una organización	Si	No	Si
Metodología eficaz con prioridad para la función informatica no formalizada	Si	No	No
De acuerdo a las caracteristicas que requiere la rama Judicial de Santander y al diagnostico de la función informatica, la metodología ideal es COBIT			

Una vez realizada la selección de la metodología se comienza a realizar el panorama de riesgo tecnológico. Pero primero veamos las etapas a cubrir:



Posteriormente empezamos con la primera etapa.

3. IDENTIFICANDO LAS CAUSAS DE RIESGO TECNOLOGICO

En esta etapa procedemos a identificar y valorar las causas de riesgo tecnológico para de esa manera tener un orden de auditaje y levantar el panorama de riesgo.

Los avances y el uso de modernas tecnologías para el procesamiento de la información y las telecomunicaciones se ven reflejados en las mejoras que realizan la mayoría de las organizaciones como la automatización de procesos, la eliminación de espacios físicos, operaciones virtuales, integración de los diferentes sistemas de información, sistemas gerenciales y el apoyo tecnológico en la ventaja estratégica.

Este impacto ha traído como consecuencia el aumento de los riesgos en la empresa originados por la dependencia del uso creciente de la tecnología, el incremento drástico en el procesamiento electrónico de datos, el tener menos visibilidad de las pistas de auditoría, a la segregación de las funciones hombre – máquina con nuevas funciones y recursos a auditar.

En la actualidad el surgimiento de nuevas tecnologías de información continúa su avance y expansión para satisfacer las nuevas demandas, necesidades de información y su funcionalidad. La prueba de esto se puede ver en el surgimiento de redes de área local, sistemas de administración de bases de datos, poderosos microcomputadores y las telecomunicaciones. Estas tecnologías han producido nuevos y adicionales riesgos y consideraciones de control, con implicaciones para la auditoria.

A la hora de levantar el panorama de riesgo tecnológico debemos tener en cuenta las siguientes causas de riesgo tecnológico:

1) SANCIONES LEGALES

Entre las sanciones legales en la rama judicial encontramos:

Uso de software no licenciado, descargas de cualquier multimedia sin autorización del autor.

Retención indebida de aportes fiscales recaudados por la empresa por fallas en sistemas de información.

Omisión del recaudo de aportes fiscales o parafiscales para los diferentes entes de control por fallas en sistemas de información.

ACTOS MAL INTENCIONADOS DE LA EMPRESA
Omitir recaudos obligados por la ley.

Recaudar impuestos inferiores a las establecidas en la ley.

No disponibilidad de los sistemas de computador para producir reportes exigidos por la ley.

ERRORES DE LA EMPRESA Y DE LOS EMPLEADOS. (ESTOS CASOS PUEDE SER FORTUITOS O ACCIDENTALES)
No enviar reportes a las entidades del gobierno en las fechas establecidas.

Errores en el cálculo de impuestos recaudados.

Errores en el cálculo de aportes parafiscales y en general de los sistemas de información.

2) HURTO/ FRAUDE

El robo de información y datos electrónicos es hoy más frecuente que el hurto de activos físicos en las empresas y algo que llama más la atención es que en la gran mayoría de las empresas que lograron identificar al culpable de los fraudes, encuentran que eran personas que trabajaban o estuvieron vinculadas a su compañía.

La empresa debe establecer políticas de seguridad y concienciación del empleado que trabaja en la misma, también es muy conocido que en las empresas existen controles y documentos que realmente no son efectivos. La empresa debe estar evaluando sus políticas hacia el personal que labora en la empresa porque la buena fe de los empleados está condicionada a las circunstancias, problemas personales, familiares, económicos, concentración de funciones, baja moral de los empleados y otras que a veces la empresa desconoce y esto de alguna manera afecta la estabilidad del empleado y lo lleva a cometer hurtos y fraudes. Adicionalmente las empresas deben establecer controles para evitar el acceso a personas no autorizadas y que de esta manera se pueda cometer hurtos y fraudes por parte de personas ajenas a la empresa, tanto en el aspecto físico como lógico, entre otros también existe la forma de buscar cómo obtener información por medio de la ingeniería social a personas claves de las empresas.

3) Daño o destrucción de activos

La organización debe velar por implementar acciones que tiendan a minimizar los riesgos a que puedan estar expuestos los activos de la compañía, o causas de riesgo como:

DAÑO Y DESTRUCCIÓN DE ACTIVOS: Que son ocasionados por desastres naturales y algunas causas que originan estos hechos son:
Terremoto y maremotos
Inundaciones
Erupciones volcánicas
Vientos o huracanes
Rayos.

ACTOS MAL INTENCIONADOS DE TERCEROS: Estos hechos se pueden presentar de acuerdo a la seguridad en que se encuentre la ciudad o sitio donde se encuentra ubicada la empresa. Se pueden presentar los siguientes hechos:
Actos terroristas
Asaltos
Vandalismo
Disturbios civiles
Virus de computador
Sabotaje de terceros que intervienen en la presentación de servicios de la empresa.

ACTOS MAL INTENCIONADOS DE LOS EMPLEADOS: Son actos que pueden llegar a suceder debido a que pueden haber empleado insatisfecho o que no está de acuerdo con algunas políticas o condiciones de la empresa. Estos actos son:

Sabotaje de empleados que intervienen en la prestación de servicios de la empresa.
Paros laborales
Cese de actividades
Daños y desastres a propósito causado por los empleados.

ACTOS ACCIDENTALES (CASOS FORTUITOS)

Inapropiadas instalaciones eléctricas.
Inapropiadas instalaciones físicas
Mal funcionamientos de los equipos de oficina

4) EXCESO DE EGRESOS

Las empresas pueden reducir sus costos si establecen políticas e implementan estándares para el hardware, interfaces de usuarios, aplicaciones, infraestructura y procesos. La empresa debe considerar y evaluar algunas prácticas en el departamento de informática para minimizar los riesgos y excesos de recursos monetarios de esta, a continuación, relacionamos algunos mecanismos para reducir el exceso de egresos por causas de riesgo asociados a tecnología:

Maximizar procesador y capacidad de almacenamiento
Remover las partes innecesarias del sistema
Revisar cálculos de los sistemas e información para su correcta ejecución.
Utilizar herramientas de administración de software, integradas
Automatizar la administración del sistema, almacenamiento y tareas operativas
Limitar la capacidad de los usuarios
Mantener inventarios de todo el hardware y software
Entrenar a los empleados
Reemplazar las aplicaciones obsoletas
Mantener la infraestructura confiable
Velar por la calidad de la información

5) Pérdida de ingresos

La pérdida de ingresos puede ocurrir debido a discrepancias en la información o pérdida de registros asignados de clientes o servicios en los diferentes sistemas y plataformas, provocando las inconsistencias entre el estado real del servicio y el estado del servicio facturado. Estas pérdidas de ingresos por falta de integridad se identifican extrayendo y reconciliando la información de configuración de varias fuentes de información.

Los problemas más frecuentes que enfrentan las organizaciones en sus procesos de generación de ingresos y que son atacados en un proceso de aseguramiento de ingresos pueden ser:

Estrategia de precios y promociones
Ventas y mercadeo
Activación
Planificación y operación de la red

Servicio al cliente
Facturación
Cobranzas
Contabilidad
Actualización tardía de información como precios y otros

La empresa debe establecer políticas y controles que permitan el aseguramiento de ingresos de una forma oportuna y eficiente. El personal debe estar capacitado para detectar las pérdidas de ingreso y costos, cuantificarlas y recuperarlas, implementando controles para que las pérdidas no vuelvan a ocurrir.

6) DESVENTAJA COMPETITIVA

La tecnología es un diferenciador ante la competencia, ya sea porque se tiene un sistema de información original o más robusto, que provee información clave para la toma de decisiones, o porque se usa tecnología como la robótica u otra para mejorar procesos, reducir costos o aumentar la calidad de los productos. Es muy importante que la empresa establezca unas políticas de cómo aumentar la competitividad y se podría lograr implementando algunos controles como son:

Divulgación accidental de información que constituye ventaja competitiva.
Interrupciones accidentales del servicio por daños en los sistemas de computador.
Obsolescencia tecnológica.
Mala atención de los clientes por parte de los empleados.
Mala calidad de los servicios ofrecidos a los clientes.
Divulgar accidentalmente información financiera sobre el estado de la empresa, por ejemplo, en impresos de uso interno.
No innovar en cuanto al desarrollo de sistemas de información
No estar actualizado con respecto a la tecnología de hardware desarrollada para la industria en que se trabaja.
En la actualidad las organizaciones buscan estar a la vanguardia, brindar el mejor servicio y /o producto utilizando tecnología de punta y a su vez tiene implícito el riesgo que debe identificar para tener controles que minimicen el impacto a la desventaja competitiva frente a las empresas similares.

7) PÉRDIDA DE IMAGEN PÚBLICA

La prestación de los servicios por internet, la actualización de las páginas web, la divulgación de la empresa por las redes sociales, las noticias de los productos o servicios de la empresa en internet, y en general la apertura a las comunicaciones globales pone en mayor riesgo a las empresas porque se encuentra expuesta a situaciones difíciles de controlar, debido a los volúmenes de las transacciones y a la cantidad de personas que pueden estar involucradas.

Algunas características de situaciones que se pudieran presentar o causas de riesgo, son:

Paros laborales, sabotajes y cese de actividades de los empleados.
Prestar servicios de mala calidad a los clientes.
Servicio inoportuno y demorado a los clientes.
Dar versiones inexactas de la situación de la empresa.
Incumplimiento y engaño a los clientes.
Violar privacidad y buen nombre de los clientes.
Inexactitud de la información entregada a los clientes
Interrupciones en las líneas de comunicación.
Interrupciones en los servicios del computador.

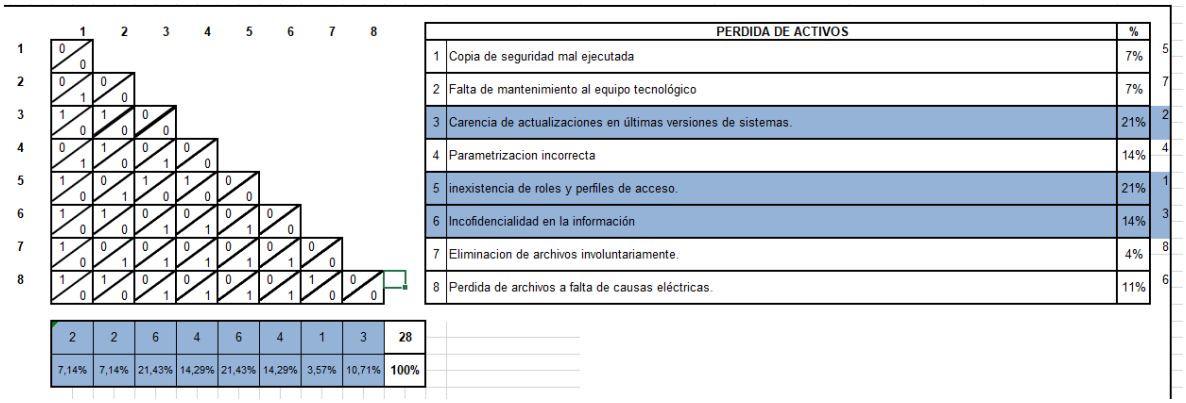
8) La toma de decisiones es una tarea compleja, puesto que más allá de la decisión presente, están las consecuencias y los riesgos futuros. Si la administración de la empresa toma decisiones basadas en elevadas expectativas corre el riesgo de fracasar, mientras que, si decide pensando en las consecuencias, entonces correrá el riesgo de no atender a oportunidades. Tomar decisiones tiene riesgos, una adecuada gestión del riesgo conlleva a que la empresa que toma decisiones deba evaluar y considerar los aspectos como la calidad de la información generada por los sistemas de información de la misma, la exacta definición de los escenarios, la actualización constante de la información y demás.

3.1 VALORACIÓN DEL RIESGO

Después de haber identificado las causas de riesgo procedemos a darle una valoración mediante la metodología Delphi.

Con la valoración lo que se logra es identificar cual causa de riesgo debe ser prioritaria para la empresa o entidad.

Los evaluadores hacen una comparación entre todas las causas de riesgo y determinan cual es de mayor importancia para posteriormente realizar la matriz de riesgo.

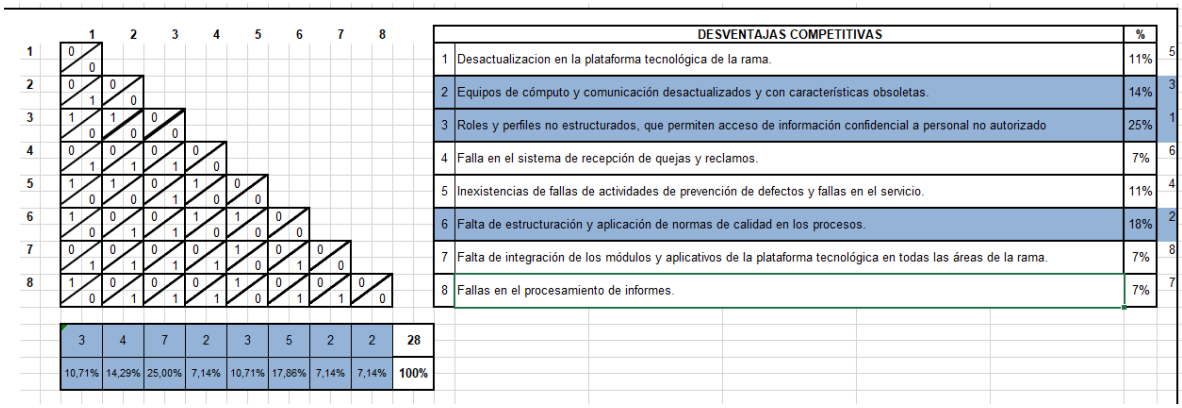


	PERDIDA DE ACTIVOS	%	
1	Copia de seguridad mal ejecutada	7%	5
2	Falta de mantenimiento al equipo tecnológico	7%	7
3	Carencia de actualizaciones en últimas versiones de sistemas.	21%	2
4	Parametrizacion incorrecta	14%	4
5	inexistencia de roles y perfiles de acceso.	21%	1
6	Incofidencialidad en la información	14%	3
7	Eliminacion de archivos involuntariamente.	4%	8
8	Perdida de archivos a falta de causas eléctricas.	11%	6

2	2	6	4	6	4	1	3	28
7,14%	7,14%	21,43%	14,29%	21,43%	14,29%	3,57%	10,71%	100%

Tabla que muestra la valoración dada a cada uno de los riesgos que pueden generar perdida de activos en la rama judicial de Santander.

Entre las causas con mayor riesgo se pueden encontrar carencia de actualizaciones en últimas versiones de software e inexistencia de roles y perfiles de acceso provocando Incofidencialidad de la información.

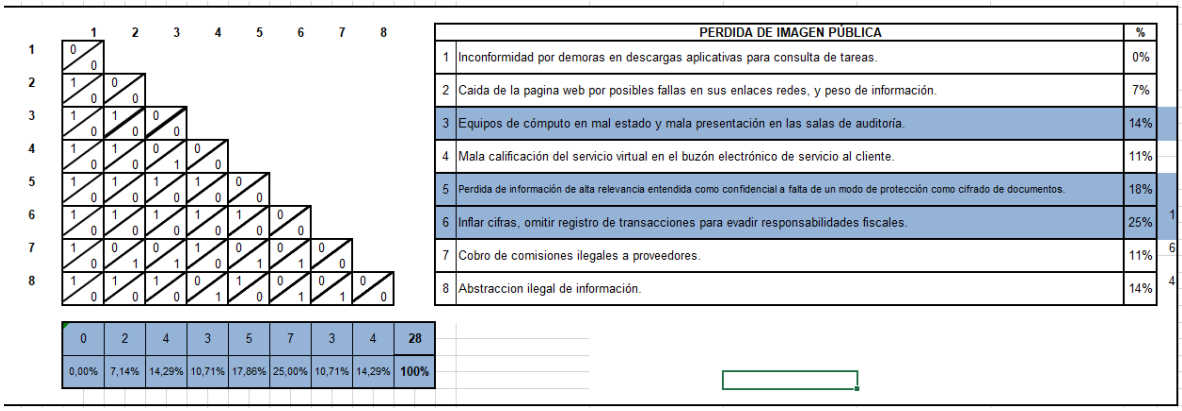


	DESVENTAJAS COMPETITIVAS	%	
1	Desactualizacion en la plataforma tecnológica de la rama.	11%	5
2	Equipos de cómputo y comunicación desactualizados y con características obsoletas.	14%	3
3	Roles y perfiles no estructurados, que permiten acceso de información confidencial a personal no autorizado	25%	1
4	Falla en el sistema de recepción de quejas y reclamos.	7%	6
5	Inexistencias de fallas de actividades de prevención de defectos y fallas en el servicio.	11%	4
6	Falta de estructuración y aplicación de normas de calidad en los procesos.	18%	2
7	Falta de integración de los módulos y aplicativos de la plataforma tecnológica en todas las áreas de la rama.	7%	8
8	Fallas en el procesamiento de informes.	7%	7

3	4	7	2	3	5	2	2	28
10,71%	14,29%	25,00%	7,14%	10,71%	17,86%	7,14%	7,14%	100%

Tabla que muestra la valoración dada a cada uno de los riesgos que pueden generar desventajas competitivas en la rama judicial de Santander.

Entre las principales causas que pueden generar riesgo encontramos equipos de cómputo desactualizados y roles y perfiles no estructurados.

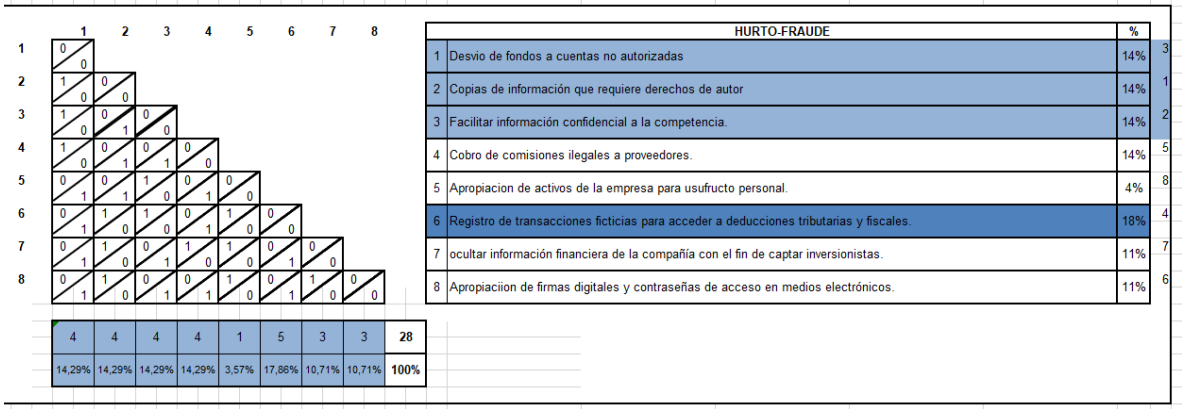


	PERDIDA DE IMAGEN PÚBLICA	%	
1	Inconformidad por demoras en descargas aplicativas para consulta de tareas.	0%	
2	Caida de la pagina web por posibles fallas en sus enlaces redes, y peso de información.	7%	
3	Equipos de cómputo en mal estado y mala presentación en las salas de auditoría.	14%	
4	Mala calificación del servicio virtual en el buzón electrónico de servicio al cliente.	11%	
5	Perdida de información de alta relevancia entendida como confidencial a falta de un modo de protección como cifrado de documentos.	18%	
6	Inflar cifras, omitir registro de transacciones para evadir responsabilidades fiscales.	25%	1
7	Cobro de comisiones ilegales a proveedores.	11%	6
8	Abstraccion ilegal de información.	14%	4

0	2	4	3	5	7	3	4	28
0,00%	7,14%	14,29%	10,71%	17,86%	25,00%	10,71%	14,29%	100%

Tabla que muestra la valoración dada a cada uno de los riesgos que pueden generar perdida de imagen pública en la rama judicial de Santander.

Entre las principales causas que pueden generar riesgo encontramos mala presentación de las salas de auditoría.

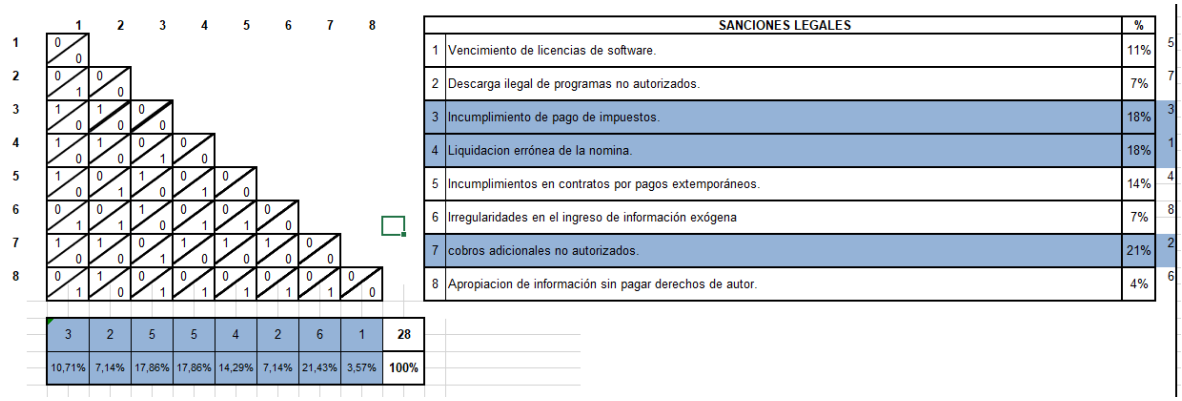


	HURTO-FRAUDE	%	
1	Desvio de fondos a cuentas no autorizadas	14%	3
2	Copias de información que requiere derechos de autor	14%	1
3	Facilitar información confidencial a la competencia.	14%	2
4	Cobro de comisiones ilegales a proveedores.	14%	5
5	Apropiacion de activos de la empresa para usufructo personal.	4%	8
6	Registro de transacciones ficticias para acceder a deducciones tributarias y fiscales.	18%	4
7	ocultar información financiera de la compañía con el fin de captar inversionistas.	11%	7
8	Apropiaciion de firmas digitales y contraseñas de acceso en medios electrónicos.	11%	6

4	4	4	4	1	5	3	3	28
14,29%	14,29%	14,29%	14,29%	3,57%	17,86%	10,71%	10,71%	100%

Tabla que muestra la valoración dada a cada uno de los riesgos que pueden generar hurto o fraude en la rama judicial de Santander.

Entre las principales causas que pueden generar riesgo encontramos copias de información que no requieren derechos de autor.

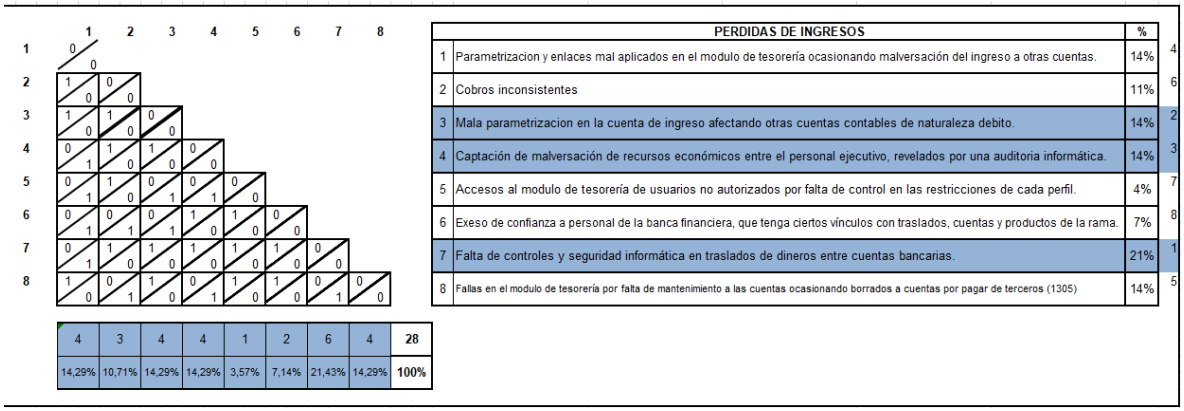


	SANCIONES LEGALES	%	
1	Vencimiento de licencias de software.	11%	5
2	Descarga ilegal de programas no autorizados.	7%	7
3	Incumplimiento de pago de impuestos.	18%	3
4	Liquidacion errónea de la nomina.	18%	1
5	Incumplimientos en contratos por pagos extemporáneos.	14%	4
6	Irregularidades en el ingreso de información exógena	7%	8
7	cobros adicionales no autorizados.	21%	2
8	Apropiacion de información sin pagar derechos de autor.	4%	6

3	2	5	5	4	2	6	1	28
10,71%	7,14%	17,86%	17,86%	14,29%	7,14%	21,43%	3,57%	100%

Tabla que muestra la valoración dada a cada uno de los riesgos que pueden generar sanciones legales en la rama judicial de Santander.

Entre las principales causas que pueden generar riesgo encontramos descarga ilegal de programas no autorizados.

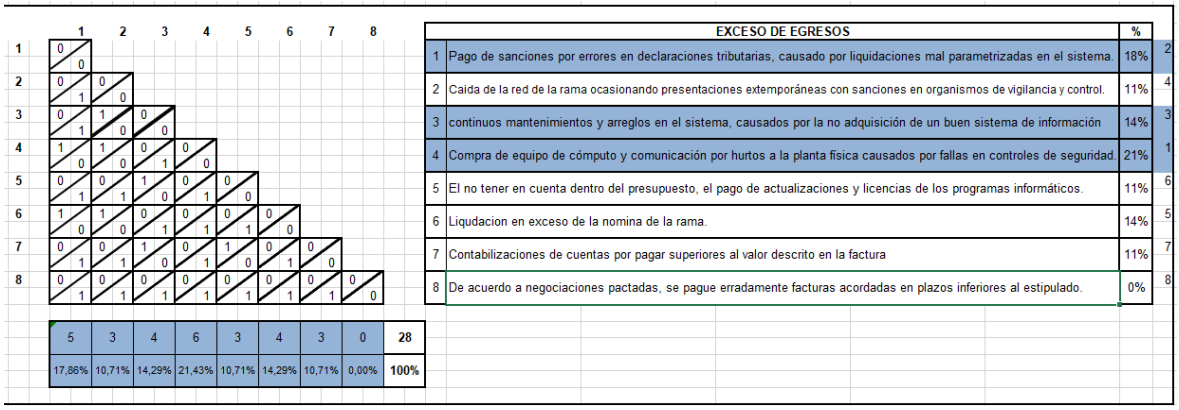


	PERDIDAS DE INGRESOS	%	
1	Parametrizacion y enlaces mal aplicados en el modulo de tesorería ocasionando malversación del ingreso a otras cuentas.	14%	4
2	Cobros inconsistentes	11%	6
3	Mala parametrizacion en la cuenta de ingreso afectando otras cuentas contables de naturaleza debito.	14%	2
4	Captación de malversación de recursos económicos entre el personal ejecutivo, revelados por una auditoria informática.	14%	3
5	Accesos al modulo de tesorería de usuarios no autorizados por falta de control en las restricciones de cada perfil.	4%	7
6	Exeso de confianza a personal de la banca financiera, que tenga ciertos vínculos con traslados, cuentas y productos de la rama.	7%	8
7	Falta de controles y seguridad informática en traslados de dineros entre cuentas bancarias.	21%	1
8	Fallas en el modulo de tesorería por falta de mantenimiento a las cuentas ocasionando borrados a cuentas por pagar de terceros (1305)	14%	5

4	3	4	4	1	2	6	4	28
14,29%	10,71%	14,29%	14,29%	3,57%	7,14%	21,43%	14,29%	100%

Tabla que muestra la valoración dada a cada uno de los riesgos que pueden generar pérdidas de ingresos en la rama judicial de Santander.

Entre las principales causas que pueden generar riesgo tenemos mala parametrización en la cuenta de acceso de JUSTICIA 21.

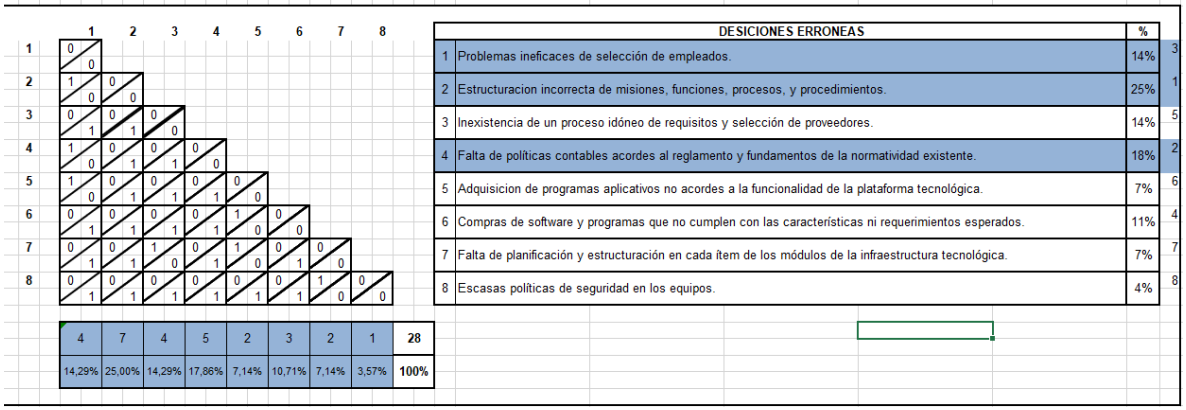


	EXCESO DE EGRESOS	%	
1	Pago de sanciones por errores en declaraciones tributarias, causado por liquidaciones mal parametrizadas en el sistema.	18%	2
2	Caida de la red de la rama ocasionando presentaciones extemporáneas con sanciones en organismos de vigilancia y control.	11%	4
3	continuos mantenimientos y arreglos en el sistema, causados por la no adquisición de un buen sistema de información	14%	3
4	Compra de equipo de cómputo y comunicación por hurtos a la planta fisica causados por fallas en controles de seguridad.	21%	1
5	El no tener en cuenta dentro del presupuesto, el pago de actualizaciones y licencias de los programas informáticos.	11%	6
6	Liqudacion en exceso de la nomina de la rama.	14%	5
7	Contabilizaciones de cuentas por pagar superiores al valor descrito en la factura	11%	7
8	De acuerdo a negociaciones pactadas, se pague erradamente facturas acordadas en plazos inferiores al estipulado.	0%	8

5	3	4	6	3	4	3	0	28
17,86%	10,71%	14,29%	21,43%	10,71%	14,29%	10,71%	0,00%	100%

Tabla que muestra la valoración dada a cada uno de los riesgos que pueden generar exceso de egresos en la rama judicial de Santander.

Entre las principales causas de riesgo que se pueden generar encontramos continuos arreglos y mantenimiento en el sistema causados por la no adquisición de un buen sistema de información.



	DESICIONES ERRONEAS	%	
1	Problemas ineficaces de selección de empleados.	14%	3
2	Estructuracion incorrecta de misiones, funciones, procesos, y procedimientos.	25%	1
3	Inexistencia de un proceso idóneo de requisitos y selección de proveedores.	14%	5
4	Falta de políticas contables acordes al reglamento y fundamentos de la normatividad existente.	18%	2
5	Adquisicion de programas aplicativos no acordes a la funcionalidad de la plataforma tecnológica.	7%	6
6	Compras de software y programas que no cumplen con las características ni requerimientos esperados.	11%	4
7	Falta de planificación y estructuración en cada ítem de los módulos de la infraestructura tecnológica.	7%	7
8	Escasas políticas de seguridad en los equipos.	4%	8

4	7	4	5	2	3	2	1	28
14,29%	25,00%	14,29%	17,86%	7,14%	10,71%	7,14%	3,57%	100%

Tabla que muestra la valoración dada a cada uno de los riesgos que pueden generar decisiones erróneas en la rama judicial de Santander.

Entre las principales causas que pueden generar riesgo encontramos compras de software y programas que no cumplen con los requerimientos esperados.

3.2 Matriz de riesgo

Posteriormente procedemos a realizar la matriz de riesgo para darle un orden de auditaje a las causas de riesgo.

ITEM	AREA	COMPONENTE	VR	%R*C	%R*A	ORDEN AUDITAJE
1	HURTO/FRAUDE	1-Desvio de fondos a cuentas no	4	14%	7%	7
		2-Copias de información que	4	14%		
		3-Facilitar información confidencial	4	14%		
		4-Cobro de comisiones ilegales a	4	14%		
		5-Apropiacion de activos de la	1	4%		
		6-Registro de transacciones ficticias	5	18%		
		7-ocultar información financiera de	3	11%		
		8-Apropiaciion de firmas digitales y	3	11%		
2	SANCIONES LEGALES	1-Vencimiento de licencias de	3	11%	11%	5
		2-Descarga ilegal de programas no	2	7%		
		3-Incumplimiento de pago de	5	18%		
		4-Liquidacion errónea de la nomina.	5	18%		
		5-Incumplimientos en contratos por	4	14%		
		6-Irregularidades en el ingreso de	2	7%		
		7-cobros adicionales no	6	21%		
		8-Apropiacion de información sin	1	4%		
3	PERDIDA DE ACTIVOS	1-Copia de seguridad mal ejecutada	2	7%	18%	3
		2-Falta de mantenimiento al equipo	2	7%		
		3-Carencia de actualizaciones en	6	21%		
		4-Parametrizacion incorrecta	4	14%		
		5-inexistencia de roles y perfiles de	6	21%		
		6-Incofidencialidad en la	4	14%		
		7-Eliminacion de archivos	1	4%		
		8-Perdida de archivos a falta de	3	11%		
4	DESVENTAJAS COMPETITIVAS	1-Desactualizacion en la plataforma	3	11%	4%	8
		2-Equipos de cómputo y	4	14%		
		3-Roles y perfiles no estructurados,	7	25%		
		4-Falla en el sistema de recepción	2	7%		
		5-Inexistencias de fallas de	3	11%		
		6-Falta de estructuración y	5	18%		
		7-Falta de integración de los	2	7%		
		8-Fallas en el procesamiento de	2	7%		

5	PERDIDA DE IMAGEN PÚBLICA	1-Inconformidad por demoras en	0	0%	18%	2
		2-Caida de la pagina web por	2	7%		
		3-Equipos de cómputo en mal	4	14%		
		4-Mala calificación del servicio	3	11%		
		5-perdida de información de alta	5	18%		
		6-Inflar cifras, omitir registro de	7	25%		
		7-Cobro de comisiones ilegales a	3	11%		
		8-Abstraccion ilegal de información	4	14%		
6	PERDIDAS DE INGRESOS	1-Parametrizacion y enlaces mal	4	12%	25%	1
		2-Cobros de matriculas	3	11%		
		3-Mala parametrizacion en la	4	14%		
		4-Captación de malversación de	4	14%		
		5-Accesos al modulo de tesorería de	1	4%		
		6-Exeso de confianza a personal de	2	7%		
		7-Falta de controles y seguridad informática en traslados de dineros	6	21%		
		8-Fallas en el modulo de tesorería	4	14%		
7	EXCESO DE EGRESOS	1-Pago de sanciones por errores en	5	18%	11%	4
		2-Caida de la red de la rama	3	11%		
		3-continuos mantenimientos y	4	14%		
		4-Compra de equipo de cómputo y	6	21%		
		5-El no tener en cuenta dentro del	3	11%		
		6-Liqudacion en exceso de la	4	14%		
		7-Contabilizaciones de cuentas por	3	11%		
		8-De acuerdo a negociaciones	0	0%		
8	DESICIONES ERRONEAS	1-Problemas ineficaces de	4	14%	6%	6
		2-Estructuracion incorrecta de	7	25%		
		3-Inexistencia de un proceso	4	14%		
		4-Falta de políticas contables	5	18%		
		5-Adquisicion de programas	2	7%		
		6-Compras de software y programas	3	11%		
		7-Falta de planificación y	2	7%		
		8-Escasas políticas de seguridad en	1	4%		
					100%	

RECOMENDACIONES

Finalmente se realizan una serie de recomendaciones para completar el proceso de auditoría.

Pérdida de ingresos

Que contabilidad trabaje en conjunto con los ingenieros o que se realice a los ingenieros en contabilidad, para que tengas las bases fundamentales mínimas para parametrizar el software.

Situación de riesgo: Fraudes

- Fracaso empresarial
- Endeudamiento

Según los Objetivos de Control para la Información y la Tecnología relacionada (COBIT®) la técnica más adecuada para establecer seria adquirir e implantar con su objetivo de control detallado de ADMINISTRAR CAMBIOS para así responder a los requerimientos del negocio de acuerdo con la estrategia, mientras se reducen los defectos y la repetición de trabajos, enfocados en controlar la evaluación de impacto, autorización e implantación de todos los cambios a la infraestructura de TI, aplicaciones y soluciones técnicas, minimizando errores que se deben a especificaciones incompletas de la solicitud y detener la implantación de cambios no autorizados. Deberán establecerse apropiadas medidas de seguridad física y control por medio de los cambios pertinentes para así evitar el doble trabajo y por consiguiente las consecuencias ya antes mencionadas

Situación de riesgo: Manipulación de las cuentas y aplicaciones del software y Exposición a pérdida del dinero.

Según los Objetivos de Control para la Información y la Tecnología relacionada (COBIT®) la técnica más adecuada es la de ADQUIRIR E IMPLEMENTAR ya que se requiere la necesidad de una nueva aplicación o función para una solución automatizada y de control, de esta técnica se tomaría como objetivo de control detallado la de Adquirir recursos de TI ya que este requiere de la definición y ejecución de los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí. El hacerlo así garantiza que la organización tenga todos los recursos de TI que se requieren de una manera oportuna y rentable, así también satisface el requisito de negocio de TI para mejorar la rentabilidad de TI y su contribución a la utilidad del negocio. enfocándose en adquirir y mantener las habilidades de TI que respondan a la estrategia de entrega, en una infraestructura TI integrada y estandarizada

Perdida de imagen publica

Asignar las salas de informática, de acuerdo a las necesidades de los diferentes tipos de usuarios, de este modo se estandariza el servicio entre las personas que tienen acceso y se exigen normas de buen uso y conservación para aumentar la vida útil de los equipos.

Cada vez que se produzca un documento de tipo confidencial a nivel judicial este sea protegido con una contraseña solo al documento de este modo las secretarias y auxiliares tienen acceso al computador de los jefes y a la información, pero no a la carpeta que se denominará confidencial y que tendrá seguridad.

Situación de riesgo: Perder publicidad.

Según los Objetivos de Control para la Información y la Tecnología relacionada (COBIT®) la técnica más adecuada es la de ENTREGAR Y DAR SOPORTE ya que se requiere la necesidad de una nueva aplicación o función para una solución automatizada y de control, de esta técnica se tomaría como objetivo de control detallado la de Educar y entrenar a los usuarios para una educación efectiva de todos los usuarios de sistemas de TI, incluyendo aquellos dentro de TI, se requieren identificar las necesidades de entrenamiento de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición y ejecución de una estrategia para llevar a cabo un entrenamiento efectivo y para medir los resultados. Un programa efectivo de entrenamiento incrementa el uso efectivo de la tecnología al disminuir los errores, incrementando la productividad y el cumplimiento de los controles clave tales como las medidas de seguridad de los usuarios, enfocándose en un claro entendimiento de las necesidades de entrenamiento de los usuarios de TI, la ejecución de una efectiva estrategia de entrenamiento y la medición de resultados. se logra con • Establecer un programa de entrenamiento • Organizar el entrenamiento • Impartir el entrenamiento • Monitorear y reportar la efectividad del entrenamiento.

Situación de riesgo:

-Pérdida de ingresos
-Devaluación de activos

Recomendación: Según los Objetivos de Control para la Información y la Tecnología relacionada (COBIT®) la técnica más adecuada es la de ADQUIRIR E IMPLEMENTAR ya que se requiere la necesidad de una nueva aplicación o función para una solución automatizada y de control, de esta técnica se tomaría como objetivo de control detallado la Adquirir y mantener software aplicativo las aplicaciones deben estar disponibles de acuerdo con los requerimientos del negocio. Este proceso cubre el diseño de las aplicaciones, la inclusión apropiada de controles aplicativos y requerimientos de seguridad, y el desarrollo y la configuración en sí de acuerdo a los estándares. Esto permite a las organizaciones apoyar la operatividad del negocio de forma apropiada con las aplicaciones automatizadas correctas. Así se mantiene un control sobre el mantenimiento al software aplicativo que satisface el requisito de negocio de TI para construir las aplicaciones de acuerdo con los requerimientos del negocio y haciéndolas a tiempo y a un costo razonable enfocándose en garantizar que exista un proceso de desarrollo oportuno y confiable

Otros objetivos de control como recomendación serían: Adquirir y mantener infraestructura tecnológica. Las organizaciones deben contar con procesos para

adquirir, implantar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio.

Adquirir recursos de TI
Se deben suministrar recursos TI, incluyendo personas, hardware, software y servicios. Esto requiere de la definición y ejecución de los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí. El hacerlo así garantiza que la organización tenga todos los recursos de TI que se requieren de una manera oportuna y rentable asi se satisface el requisito de negocio de TI para mejorar la rentabilidad de TI y su contribución a la utilidad del negocio.

Perdida de activos

Que se parametrice en el sistema una fecha previa de vencimiento de términos legales de programas. De modo que exista un lapso prudencial para que la oficina de sistemas, y las diferentes unidades académicas puedan gestionar a nivel interno el presupuesto necesario para renovar los permisos y eliminar el riesgo de que se venza el permiso para operar y no se hayan renovado la licencia legal de funcionamiento.

Realizar una configuración de perfiles para usuarios externos como administrativos o financieros, ingenieros que ingresan a los computadores, pero no deben tener acceso a la información guardada en la configuración personal y que contiene aspectos de fondo, rigurosos del quehacer diario de la Rama Judicial de Santander.

Situación de riesgo:
-Desactualizaciones tecnológicas
-Pérdida de ingresos
Recomendación:

Según los Objetivos de Control para la Información y la Tecnología relacionada (COBIT®) la técnica más adecuada es la de monitorear y evaluar y adquirir e implantar ya que se requiere la necesidad de una nueva aplicación o función para una solución automatizada y de control, de esta técnica se tomaría como objetivos de control detallado los siguientes: Adquirir y mantener infraestructura tecnológica.

Las organizaciones deben contar con procesos para adquirir, implantar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las

estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas.

Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio. Control sobre el proceso TI de:

Adquirir y dar mantenimiento a la infraestructura tecnológica que satisface el requisito de negocio de TI para adquirir y dar mantenimiento a una infraestructura integrada y estándar de TI enfocándose en proporcionar plataformas adecuadas para las aplicaciones del negocio, de acuerdo con la arquitectura definida de TI y los estándares de tecnología.

Monitorear y evaluar el desempeño de TI

Una efectiva administración del desempeño de TI requiere un proceso de monitoreo. El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones. El monitoreo se requiere para garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y políticas. Control sobre el proceso TI de Monitorear y evaluar el desempeño de TI que satisface el requisito de negocio de TI para transparencia y entendimiento de los costos, beneficios, estrategia, políticas y niveles de servicio de TI de acuerdo con los requisitos de gobierno enfocándose en monitorear y reportar las métricas del proceso e identificar e implantar acciones de mejoramiento del desempeño.

Situación de riesgo: Pérdida de información y falta de productividad.

Recomendación

Según los Objetivos de Control para la Información y la Tecnología relacionada (COBIT®) la técnica más adecuada es la de ENTREGAR Y DAR SOPORTE ya que se requiere la necesidad de una nueva aplicación o función para una solución automatizada y de control, de esta técnica se tomaría como objetivo de control detallado la de Garantizar la seguridad de los sistemas la necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas, así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.

Garantizar la seguridad de los sistemas que satisface el requisito de negocio de TI para mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de las vulnerabilidades e incidentes de seguridad. enfocándose en la definición de políticas, procedimientos y estándares de seguridad de TI y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.

CONCLUSIONES

Se debería implementar una herramienta de software que permita realizar el levantamiento de panorama de riesgo de una manera más simple y eficaz.

Trabajar con la metodología COBIT fue una gran experiencia puesto que es fácil de entender y aplicar.

El conocimiento de la función informática fue tedioso en principio puesto que no se contaba con una gestión formalizada de las TI de la rama judicial.

Trabajar con la Rama Judicial fue una experiencia gratificante puesto que es un entorno laboral comprometido y dispuesto a ayudar.

REFERENCIAS Y BIBLIOGRAFÍA

[1]F. Rojas R, Cobit 4.0 Nuevas características, 4th ed. Bogotá: ISACA, 2014, p. 38.

[2]"COBIT 4.0: Una Actualización Principal en el Estándar Internacional Permite a las Empresas Aumentar su Valor IT y Reducir los Riesgos", Isaca.org, 2018. [Online]. Available: https://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/COBIT-4-0-Una-actualizacion-principal-en-el-estandar-internacional-permite-a-las-empresas-aumentar-s.aspx. [Accessed: 19- Aug- 2018].

[3]Pegasus.javeriana.edu.co. [Online]. Available: http://pegasus.javeriana.edu.co/~CIS1210IS02/news/Gu%C3%ADa%20Metodol%C3%B3gica%20para%20COBIT%204.1.pdf. [Accessed: 22- Aug- 2018].

[4]E. Business, "Los cinco principios de COBIT 5", Esan.edu.pe, 2016. [Online]. Available: https://www.esan.edu.pe/apuntes-empresariales/2016/06/los-cinco-principios-de-cobit-5/. [Accessed: 24- Aug- 2018].

[5]D. Soto, "¿Qué es Cobit y para qué sirve? - Principios de Cobit 5", Nextech Education Center, 2016. [Online]. Available: https://nextech.pe/que-es-cobit-y-para-que-sirve/. [Accessed: 27- Aug- 2018].

[6]"Metodología ITIL, 'la biblioteca' que adapta las empresas al mundo digital", Coremain, 2018. [Online]. Available: http://www.coremain.com/metodologia-itil/. [Accessed: 25- Aug- 2018].

[7]F. Donoso and P. Ramirez Bravo, "Metodología ITIL", Repositorio.uchile.cl, 2006. [Online]. Available: http://repositorio.uchile.cl/bitstream/handle/2250/108405/donoso_f.pdf?sequence=3&isAllowed=y. [Accessed: 13- Sep- 2018].

[8]J. Acevedo, "Esto es lo que están buscando los departamentos de seguridad", PC World en Español, 2015. [Online]. Available: http://www.pcworldenespanol.com/2015/09/25/asi-es-el-perfil-profesional-que-buscan-las-empresas-para-sus-departamentos-de-seguridad-informatica/. [Accessed: 10- Oct- 2018].

[9]J. Edge, "CISA Salario: ¿Cuánto puede ganar? - CRUSH The InfoSec ExamS August 23, 2018", Aplastar a los exámenes InfoSec, 2018. [Online]. Available: https://crushtheinfosecexams.com/cisa-salary/?lang=es. [Accessed: 25- Oct- 2018].

[10]"Riesgo Tecnológico - Idiger", Idiger.gov.co, 2018. [Online]. Available: http://www.idiger.gov.co/rtecnologico. [Accessed: 16- Sep- 2018].

[11]A. Ramirez Castro, "Riesgo tecnológico y su impacto para las organizaciones parte I | Revista .Seguridad", Revista.seguridad.unam.mx, 2018. [Online]. Available: https://revista.seguridad.unam.mx/numero-14/riesgo-tecnol%C3%B3gico-y-su-impacto-para-las-organizaciones-parte-i. [Accessed: 23- Sep- 2018].
[12]K. Rodríguez, "Riesgo tecnológico. Su medición como prioridad para el aseguramiento del negocio", Auditool.org, 2011. [Online]. Available: https://www.auditool.org/blog/auditoria-de-ti/827-riesgo-tecnologico-su-medicion-como-prioridad-para-el-aseguramiento-del-negocio. [Accessed: 16- Oct- 2018].
[13]D.García, "Cómo elaborar una Matriz de Riesgos - EALDE Business School", EALDE Business School, 2017. [Online]. Available: https://www.ealde.es/como-elaborar-matriz-de-riesgos/. [Accessed: 10- Aug- 2018].
[14]"¿En qué consiste una matriz de riesgos?", Software ISO, 2015. [Online]. Available: https://www.isotools.org/2015/08/06/en-que-consiste-una-matriz-de-riesgos/. [Accessed: 22- Sep- 2018].
[15]G. Colombia, "Todo lo que necesitas saber sobre la Auditoría de sistemas de información. - Grant Thornton Colombia", Grant Thornton Colombia, 2017. [Online]. Available: http://blog.grantthornton.com.co/actualidad/todo-lo-que-necesitas-saber-sobre-la-auditoria-de-sistemas-de-informacion/. [Accessed: 25- Oct- 2018].
[16]A. Rojo, "Las cualidades de un auditor de sistemas de gestión", SBQ Consultores, 2015. [Online]. Available: https://www.sbqconsultores.es/las-cualidades-de-un-auditor/. [Accessed: 21- Sep- 2018].
[17]"¿Cuáles son las cualidades que debe tener un auditor ISO 27001?", Isotools.com.mx, 2017. [Online]. Available: https://www.isotools.com.mx/cuales-las-cualidades-auditor-iso-27001/. [Accessed: 20- Aug- 2018].
[18]R. Toro, "10 pasos para elaborar una matriz de riesgos laborales", Nueva ISO 45001, 2018. [Online]. Available: https://www.nueva-iso-45001.com/2018/03/matriz-de-riesgos/. [Accessed: 25- Oct- 2018].
[19]"Publicada la nueva norma ISO 19011:2018 - Directrices para la auditoría de sistemas de gestión - Escuela Europea de Excelencia", Escuela Europea de Excelencia, 2018. [Online]. Available: https://www.escuelaeuropeaexcelencia.com/2018/08/publicada-la-nueva-norma-iso

-19011-2018-directrices-para-la-auditoria-de-sistemas-de-gestion/. [Accessed: 25- Sep- 2018].
[20]J. Lopez Patiño, "ISO 19011:2018, la nueva guía de auditoría para auditar los sistemas de gestión de las organizaciones. | Visión Industrial", ISO 19011:2018, la nueva guía de auditoría para auditar los sistemas de gestión de las organizaciones. | Visión Industrial, 2018. [Online]. Available: http://www.visionindustrial.com.mx/industria/calidad/iso-190112018-la-nueva-guia-de-auditoria-para-auditar-los-sistemas-de-gestion-de-las-organizaciones. [Accessed: 18- Oct- 2018].
[21]Ramajudicial.gov.co. [Online]. Available: https://www.ramajudicial.gov.co/. [Accessed: 26- Aug- 2018].
[22]"Organigrama del estado Colombiano-Rama Judicial", C-politica.uniandes.edu.co. [Online]. Available: https://c-politica.uniandes.edu.co/oec/index.php?ac=rj&main=4&id=1&dat=15. [Accessed: 13- Sep- 2018].
[23]S. Acosta Lozano and R. Perdomo González, "Palacio de Justicia | Patrimonio Urbano de Bucaramanga", Patrimonio Urbano de Bucaramanga. [Online]. Available: http://historiaabierta.org/mapa/items/show/20. [Accessed: 25- Aug- 2018].
[24]"Técnicas de Evaluación de Riesgos - Técnica de evaluación Delphi.", Auditool, 2014. [Online]. Available: https://www.auditool.org/blog/control-interno/2569-tecnicas-de-evaluacion-de-riesgos-tecnica-de-evaluacion-delphi. [Accessed: 22- Sep- 2018].
[25]"Método Delphi", Byte10.blogspot.com, 2010. [Online]. Available: http://byte10.blogspot.com/2010/10/metodo-delphy.html#more. [Accessed:12- Oct- 2018].
[26]J. Calle, "Etapas y fases de la auditoría interna", Riesgoscero.com, 2018. [Online]. Available: https://www.riesgoscero.com/blog/etapas-y-fases-de-la-auditoria-interna. [Accessed: 20- Aug- 2018].
[27]M. Becher, "Las 4 etapas esenciales en auditorías de calidad", SoftExpert Excellence Blog, 2017. [Online]. Available: https://blog.softexpert.com/es/las-4-etapas-esenciales-en-auditorias-de-calidad/. [Accessed: 09- Sep- 2018].
[28]C. Moncayo, "Importancia de la auditoría en los sistemas de gestión - Instituto Nacional de Contadores Públicos de Colombia", Instituto Nacional de Contadores Públicos de Colombia, 2016. [Online]. Available: https://www.incp.org.co/importancia-de-la-auditoria-en-los-sistemas-de-gestion/.

[Accessed: 28- Sep- 2018].
[29]M. HUCHANI, "IMPORTANCIA DE AUDITORIA INFORMATICA EN UNA EMPRESA", Academia.edu. [Online]. Available: https://www.academia.edu/10886388/IMPORTANCIA_DE_AUDITORIA_INFORMATICA_EN_UNA_EMPRESA?auto=download. [Accessed: 25- Oct- 2018].
[30]"Los 6 principales tipos de sistemas de información", El blog de Kyocera: soluciones para digitalizar tu negocio, 2017. [Online]. Available: http://smarterworkspaces.kyocera.es/blog/los-6-principales-tipos-sistemas-informacion/. [Accessed: 22- Oct- 2018].