AUDITORÍA A LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA EXPRESO JUANAMBÚ DE LA CIUDAD DE PASTO SOPORTADA EN LOS ESTÁNDARES DE AUDITORÍA COBIT E ISO/IEC 27000

ALVARO RONALD ERASO CERÓN
IVAN DAVID GUERRERO ARELLANO

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2015

AUDITORÍA A LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA EXPRESO JUANAMBÚ DE LA CIUDAD DE PASTO SOPORTADA EN LOS ESTÁNDARES DE AUDITORÍA COBIT E ISO/IEC 27000

ÁLVARO RONALD ERASO CERÓN
IVAN DAVID GUERRERO ARELLANO

Trabajo de grado presentado como requisito parcial para optar al título de Ingeniero de Sistemas

Director:
MSc. (C) JOSÉ JAVIER VILLALBA ROMERO
Co-Director:
Ing. FRANCISCO NICOLÁS SOLARTE SOLARTE

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2015

NOTA DE RESPONSABILIDAD

”La Universidad de Nariño no se hace responsable de las opiniones o resultados obtenidos en el presente trabajo y para su publicación priman las normas sobre el derecho de autor.”

Artículo 13, acuerdo No. 005 de 2010, emanado del Honorable Consejo Académico de la Universidad de Nariño.

“Las ideas y conclusiones aportadas en el siguiente trabajo son responsabilidad exclusiva del autor.”

Artículo 1ro del Acuerdo No. 324 de octubre 11 de 1966 emanado del Honorable Consejo Directivo de la Universidad de Nariño.

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del Director

_____

Firma del Jurado

_____

Firma del Jurado

San Juan de Pasto, 26 de octubre de 2015

AGRADECIMIENTOS

Los integrantes de este trabajo de grado queremos expresar nuestros más sinceros agradecimientos:

A nuestros asesores, Ingeniero Javier Villalba e Ingeniero Francisco Solarte, por sus ideas, asesorías y recomendaciones, por toda su sabiduría compartida en este proyecto de grado y de igual manera agradecimientos especiales al Ingeniero Nelson Jaramillo, por su motivación hacia nosotros para salir adelante en todo el transcurso de la carrera.

A las personas que integran Expreso Juanambú, a sus directivos por su confianza, por su gran colaboración, por abrir las puertas de su organización.

Queremos agradecer a todas las personas que compartieron sus conocimientos; a la Universidad de Nariño, profesores, estudiantes, amigos y demás conocidos.

DEDICATORIA

A la vida porque a pesar de todos los obstáculos, y cada vez que sentía que debía desistir, siempre puso una puerta a la salida de todos los problemas que se cruzaron por mi camino.

A mis padres, porque a pesar de las grandes dificultades, siempre me alentaron a continuar adelante. Ejemplo de superación, de nobleza y humildad.

A mis hijos, que fueron el principal motor de la lucha diaria, en especial mi hija mayor, por su compañía, por su gran apoyo incondicional, alentándome para salir adelante, continuar superándome y poder brindar un futuro mejor para ellos.

A mi compañero de trabajo de grado, que con sus conocimientos fue apoyo fundamental en el transcurso de la carrera y en la culminación de este proyecto.

ALVARO RONALD ERASO CERÓN

DEDICATORIA

A mis padres y a mi hermana, por su gran ejemplo de superación y todo el apoyo brindado a lo largo de esta carrera, el camino fue largo, pero gracias a ustedes salí adelante y solo por ustedes seguiré esforzándome para conseguir todas mis metas.

A mis familiares y amigos que siempre creyeron en mí, me brindaron consejos, me dieron fortaleza para continuar y me brindaron su amistad y cariño.

A las personas que ya no se encuentran conmigo, todas ustedes fueron parte de mi vida y siempre los recordare y los llevare en mi corazón por todos los momentos compartidos.

IVAN DAVID GUERRERO ARELLANO

RESUMEN

El desarrollo de este trabajo, realizó la auditoría a la seguridad de la información en la empresa Expreso Juanambú ubicada en la ciudad de Pasto, una empresa dedicada al servicio de transporte urbano de pasajeros.

El propósito de esta auditoría fue verificar el funcionamiento de la empresa utilizando estándares internacionales de auditoría y la metodología MAGERIT para el análisis de riesgos.

Este trabajo consta de seis capítulos. En el primer capítulo se definió cual es el problema presentado en la empresa Expreso Juanambu y se plantearon los objetivos de la investigación. En el segundo capítulo se hizo un resumen de los principales aspectos teóricos de los temas tratados en el trabajo. En el tercer capítulo se definió la metodología utilizada para el desarrollo de la auditoría. En el cuarto capítulo se expresó algunos resultados obtenidos en el proceso de auditoría. En el quinto capítulo se realizó las conclusiones del trabajo de grado y en el sexto capítulo se hizo algunas recomendaciones para futuros trabajos de este tipo.

ABSTRACT

The development of this work, carried out the audit of information security in the company Expreso Juanambú located in the city of Pasto, a company dedicated to the service of urban transport of passenger.

The purpose of this audit was to verify the performance of the company using international standards of auditing and the MAGERIT methodology for risk analysis.

This work consists of six chapters. In the first chapter was defined which is the problem is presented in the company Expreso Juanambu and raised the research objectives. The second chapter summarizes the main theoretical aspects of the topics covered in the work was done. In the third chapter the methodology used for the development of the audit was defined. In the fourth chapter some results of the audit process was expressed. In the fifth chapter the conclusions of the research work was performed and in the sixth made some recommendations for future work of this kind.

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

TABLA DE FIGURAS

Pág.

TABLA DE ANEXOS

GLOSARIO

CHECKLIST: lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo.

ESTÁNDAR: es toda regla aprobada o práctica requerida para el control de la performance técnica y de los métodos utilizados por el personal involucrado en el planeamiento y análisis de los sistemas de información.

INFORME DE AUDITORÍA: es el producto final del auditor y un medio formal de comunicar los objetivos de la auditoría, el cuerpo de las normas de auditoría que se utilizan, el alcance de auditoría, y los hallazgos y conclusiones.

METODOLOGÍA: es un conjunto de etapas formalmente estructuradas, de manera que brinden a los interesados los siguientes parámetros de acción en el desarrollo de sus proyectos: plan general y detallado, tareas y acciones, tiempos, aseguramiento de la calidad, involucrados, etapas, revisiones de avance, responsables, recursos requeridos, etc.

INTRODUCCIÓN

En los últimos años la información ha venido convirtiéndose en la parte más importante de una organización. Es por eso que hay que crear mecanismos y/o procesos que aseguren su integridad, ya que a causa de la globalización está en gran peligro y está sufriendo de grandes amenazas en cuanto a su confiabilidad y resguardo.

Es también obligación de las organizaciones lograr mayor seguridad en el manejo y procesamiento de la información que garanticen disponibilidad, integridad, confidencialidad, confiabilidad y buen desempeño mediante la implementación de un sistema de control interno a nivel técnico administrativo y físico. Para cumplir este objetivo es necesario que las organizaciones se apoyen en estándares nacionales e internacionales que se va a utilizar a lo largo del desarrollo de este trabajo.

Para hablar de seguridad se tuvo en cuenta la ISO/IEC 27000, es una norma adecuada para cualquier organización, grande o pequeña de cualquier sector, ya que hace énfasis en la protección de la información y proporciona una metodología para la implementación de la seguridad de la información en una organización.

En el caso de este proyecto se aplicaron procesos de auditoría que resguardan la información de la Empresa Expreso Juanambú, una empresa que está migrando a nuevas tecnologías de la información y generando así la prestación de nuevos servicios para sus clientes. Los estándares que se aplicaron son los siguientes: para análisis de riesgos MAGERIT, para elección de los procesos a auditar COBIT y para control de seguridad de la información ISO/IEC 27000.

El proyecto se enfocó en realizar la auditoría a la empresa Expreso Juanambú de la ciudad de Pasto, específicamente a la seguridad de la información, se identificaron diferentes hallazgos y vulnerabilidades en la seguridad física y lógica a las cuales se encuentra expuesta la información que se maneja diariamente, se evaluó sus entradas, procedimientos, controles, archivos y seguridad, y se generó un informe de recomendaciones para que haya una utilización más eficiente y segura de la información.

ELEMENTOS DE IDENTIFICACIÓN

PLANTEAMIENTO DEL PROBLEMA

La información dentro de la organización está expuesta a diferentes tipos de vulnerabilidades y amenazas que pueden impactar el buen nombre de la empresa afectando económicamente y haciendo que sus procesos y servicios sean poco confiables perdiendo credibilidad entre sus clientes.

Algunos problemas presentes en la empresa Expreso Juanambú son los siguientes:

- No existe un plan estratégico de sistemas.
- No se realiza análisis de riesgo a los cargos del personal de informática.
- Los servidores y otros equipos importantes para la empresa, no cuentan con un mantenimiento preventivo y correctivo.
- No todo el software instalado en la compañía cuenta con su respectiva licencia de uso.
- No se tiene estrictamente prohibido a los usuarios instalar software en los equipos
- No se verifica periódicamente que los usuarios no hayan instalado software en sus equipos.

- No se realizan pruebas periódicamente a las copias de respaldo, para asegurar que estén correctas y completas.
- No existe un plan de contingencia, que permita la continuidad de las operaciones fundamentales.
- El acceso al centro de cómputo está permitido para el personal autorizado.
- El área del centro de cómputo no cuenta con medidas adecuadas de seguridad (control de acceso, controles de humedad, humo, temperatura, lugar limpio e iluminado).
- No se encuentran cerca al centro de cómputo extintores especiales para equipos.
- No se realiza mantenimiento de las UPS.

Los servicios prestados por Expreso Juanambú nunca han sido sometidos a procesos formales para identificar vulnerabilidades de la información en las instalaciones de manera lógica, física, tecnológica y de software.

La empresa no se ha preocupado por garantizar la seguridad en el manejo de la información, por eso sus sistemas tienen errores y existe redundancia en datos, los cuales generan procesos lentos y repetitivos.

Las zonas destinadas para el servidor y los aparatos tecnológicos no son adecuadas, manejan un nivel de protección bajo en cuanto a seguridad y presentan problemas de inoperatividad.

FORMULACIÓN DEL PROBLEMA

¿Cómo evaluar la seguridad de la información en la empresa Expreso Juanambú, en cuanto a hardware, software e instalaciones, con procesos de auditoría que permitan establecer recomendaciones, que orienten la definición de políticas, procesos y procedimientos de la organización?

JUSTIFICACIÓN

La auditoría de sistemas es fundamental a la hora de evaluar la eficiencia y eficacia en el desempeño de la seguridad de la información, ya que proporciona controles, técnicas y procedimientos para verificar la confiabilidad del sistema, los niveles de seguridad y corregir errores.

Por lo anterior, el proceso de auditoría de sistemas se convierte en un elemento esencial y muy importante para determinar los hallazgos y vulnerabilidades más relevantes en cuanto a seguridad presentados en la empresa Expreso Juanambú.

Con la ejecución de la auditoría se benefician los usuarios de la empresa, sus directivos y la comunidad en general, ya que con base en los resultados se podrá tomar las medidas necesarias que permita optimizar los procesos de seguridad en la empresa.

La seguridad de la información es muy importante para cualquier empresa, la información que hace mucho tiempo atrás se mantenía tradicionalmente en papel, hoy se conserva en computadoras, exponiendo a que cualquier persona pueda acceder libremente a esta.

Por eso se debe garantizar que la información esté protegida. Además de prevenir que quienes no están autorizados a acceder, no lo hagan. Se debe concientizar en cuál sería el impacto negativo que podría tener un ataque informático.

Por estos motivos, la seguridad de la información sirve para garantizar la privacidad y la continuidad del servicio, tratando de minimizar la vulnerabilidad de los sistemas y de la información contenida en ellos, así como de las redes privadas y sus recursos.

Este proyecto es importante ya que se brindará recomendaciones a la empresa Expreso Juanambú para que hagan un adecuado uso de su información, para garantizar que cumplan con ciertos parámetros en seguridad de la información.

Con este proyecto no solo se beneficia la Junta Directiva, sino que cada persona involucrada en la empresa Expreso Juanambú, se sentirá segura, sabrá que contará con una empresa confiable y que administra de forma correcta todos los datos y la información de sus empleados y clientes.

La empresa Expreso Juanambú, ofrecerá a sus clientes nuevas formas de respaldar su información, garantizará el uso adecuado de seguridad de la información, atrayendo más público y compitiendo con otras empresas.

OBJETIVOS

OBJETIVO GENERAL

Evaluar la seguridad de la información en cuanto a hardware, software e instalaciones, con procesos de auditoría basada en los estándares COBIT e ISO/IEC 27000, con el propósito de establecer recomendaciones, que permitan la definición de políticas, procesos y procedimientos de la organización Expreso Juanambú.

OBJETIVOS ESPECÍFICOS

- Evaluar la seguridad de la información en cuanto a hardware, con procesos de auditoría basada en los estándares COBIT e ISO/IEC 27000, con el propósito de establecer recomendaciones, que permitan la definición de políticas, procesos y procedimientos de la organización Expreso Juanambú en este aspecto.

- Evaluar la seguridad de la información en cuanto a software, con procesos de auditoría basada en los estándares COBIT e ISO/IEC 27000, con el propósito de establecer recomendaciones, que permitan la definición de políticas, procesos y procedimientos de la organización Expreso Juanambú en este aspecto.
- Evaluar la seguridad de la información en cuanto a instalaciones, con procesos de auditoría basada en los estándares COBIT e ISO/IEC 27000, con el propósito de establecer recomendaciones, que permitan la definición de políticas, procesos y procedimientos de la organización Expreso Juanambú en este aspecto.
- Presentar el informe final de auditoría con recomendaciones soportadas en hallazgos y evidencias de la ejecución.

1. MARCO REFERENCIAL

1.1. ANTECEDENTES DE INVESTIGACIÓN

Entre los trabajos de grado realizados, relacionados con el objeto de estudio se puede mencionar los siguientes:

DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO, realizado por María Constanza Torres B. y Efraín Fajardo Guevara. El trabajo consistió en realizar los procesos de auditoría a la seguridad del Centro de Informática de la Universidad de Nariño. Este trabajo tiene relación ya que concientizó al centro de informática en definir políticas de seguridad para que sea más seguro.

AUDITORÍA DE SEGURIDAD INFORMÁTICA ISO 27001 PARA LA EMPRESA DE ALIMENTOS “ITALIMENTOS CIA. LTDA.”, realizado por Christian Miguel Cadme Ruiz y Diego Fabián Duque Pozo en la Universidad Politécnica Salesiana Sede Cuenca (Ecuador). El trabajo consistió en aplicar los procesos de auditoría a la seguridad de la empresa ITALIMENTOS CIA. LTDA. Este trabajo aplicó una norma internacional para realizar el proceso de auditoría.

AUDITORÍA INFORMÁTICA DE LA COOPERATIVA DE AHORRO Y CRÉDITO “ALIANZA DEL VALLE” LTDA. APLICANDO COBIT 4.0, realizado por Gabriela Fernanda Barros Marcillo y Andrea Erika Cadena Marten en la Universidad Escuela Politécnica del Ejército (Ecuador). El trabajo consistió en describir la Auditoría Informática de los Sistemas de Tecnología e Información, realizada a la Cooperativa de Ahorro y Crédito “Alianza del Valle”. Ltda. Utilizando COBIT, una herramienta desarrollada para, ayudar a los administradores de negocios a entender y administrar los riesgos asociados con la implementación de nuevas tecnologías, las

buenas prácticas de COBIT están enfocadas en el ambiente de control óptimo que debe tener una empresa para de esta manera lograr una alineación efectiva entre TI y los objetivos de negocio. El fin de esta revisión técnica es identificar debilidades y emitir recomendaciones que permitan minimizar riesgos.

Este trabajo de grado escogió unos dominios para ser auditados y se aplicó un marco internacional para las prácticas del control de información.

1.2. MARCO CONTEXTUAL

El 12 de junio de 1978, mediante escritura pública No. 1769 en el Circuito Notarial de Pasto, y ante el señor LAUREANO VILLOTA, notario segundo del referido circuito, se constituye legalmente, la empresa EXPRESO JUANAMBÚ S.A. con carácter de Sociedad Anónima.

EXPRESO JUANAMBÚ S.A. se constituyó como persona jurídica comercial de duración limitada y sin ánimo de lucro, con patrimonio formado por la reunión de fondos administrados, por accionistas responsables solo hasta el monto de sus respectivos aportes y con domicilio principal en la ciudad de San Juan de Pasto, con la posibilidad de establecer nuevas sucursales o agencias en las distintas ciudades del departamento o de la Republica, siempre y cuando las necesidades de la sociedad así lo requieran.

A partir del año 1995, la empresa pone en marcha el sistema de Radio Teléfono junto al servicio de mantenimiento de sus vehículos, con lo cual se produce una notable mejora del servicio, proporcionando a la empresa una mejor imagen corporativa y una mejor cobertura del mercado.

En el año 2012, se empezó a realizar un estudio de factibilidad para el mejoramiento del Servicio de Comunicaciones con la implementación e innovación de nuevas

tecnologías existentes en el mercado mundial como el Sistema GPS, que actualmente es utilizado a través de equipos tablet y celulares smartphone, que puede ofrecer una mayor satisfacción a sus clientes y mayor demanda del servicio con mejor seguridad y rentabilidad.

En el año 2015, está a la vanguardia de los cambios en el sector, manteniendo un adecuado servicio y atendiendo las necesidades de los clientes y colaboradores, haciendo uso de recursos humanos, físicos y tecnológicos, que permiten proyectar una imagen de calidad ante la comunidad.

La empresa posee unas instalaciones físicas de su propiedad donde trabajan 12 empleados directos con todas las prestaciones de Ley y más de 50 empleados indirectos, los que permiten el buen desempeño de la empresa en todos sus servicios.

1.2.1. Portafolio de servicio. Expreso Juanambú S.A. cuenta con los siguientes servicios:

- Transporte urbano de taxis
- Servicio de taxis con operación nacional
- Servicio de GPS y Radio Taxi
- Servicio complementario (taller de mantenimiento, monta llantas)

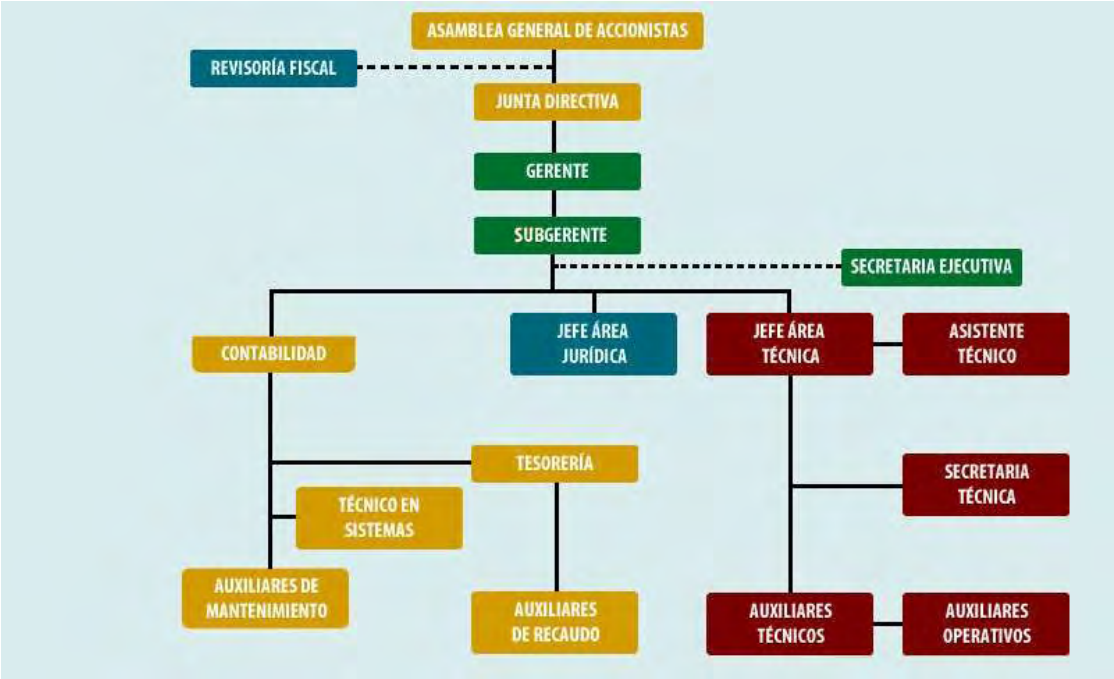
1.2.2. Misión. Prestar el servicio urbano de pasajeros orientado a la satisfacción de nuestros clientes o usuarios, buscando lograr el crecimiento, la innovación y expansión regional, contando siempre con un recurso humano, calificado y comprometido, que permita ofrecer a sus accionistas y afiliados una rentabilidad del negocio.

1.2.3. Visión. En el año 2020, seremos la mejor opción en transporte urbano, estando a la vanguardia de los cambios en el sector, manteniendo un adecuado servicio y atendiendo las necesidades de nuestros clientes y colaboradores, haciendo uso de nuestros recursos humanos, físicos y tecnológicos, que permitan proyectar una imagen de calidad ante la comunidad.

1.2.4. Estructura orgánica. La empresa Expreso Juanambú, tiene 7 áreas de trabajo las cuales están conformadas así:

- Gerencia: verificar que todos los procedimientos se cumplan correctamente.
- Secretaria: atención del cliente, recepción de documentos, cancelación de contratos, otras funciones para vehículos y propietarios del parque automotor.
- Revisoría fiscal: revisar que la contabilidad se encuentre al día y generar un dictamen sobre los estados financieros.
- Telemática: administración y mantenimiento de recursos informáticos.
- Radiocomunicaciones: asignar un servicio de taxis.
- Caja y tesorería: registra el recaudo de ingresos diariamente que se genera en la empresa.
- Lubricentro y monta llantas: mantenimiento de los vehículos.

FIGURA 1. ESTRUCTURA ORGÁNICA - EXPRESO JUANAMBÚ



1.3. MARCO TEÓRICO

La investigación se soporta en diferentes teorías y conceptos de autores que han indagado y explorado los diferentes temas acerca de la seguridad de la información, auditoría de sistemas, estándares de auditoría, entre otros. A continuación, se describe estos temas.

1.3.1. Seguridad de la información. Vieites (2007), define la seguridad informática como "Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el accesos de usuarios autorizados al sistemas"[1].

[1] GÓMEZ VIEITES, Álvaro, Enciclopedia de la seguridad informática, Alfa Omega grupo editor, México, Primera edición, 2007, pág. 4.

Kim & Solomon (2010), la confidencialidad es mantener la seguridad haciendo que solo personas autorizadas pueden ver datos protegidos, el problema de esto en las organizaciones es decidir que es confidencial y quienes tienen el acceso correcto a esto. La disponibilidad hace referencia a la condición de la información de encontrarse a disposición de quienes deben acceder a ella. La integridad busca mantener los datos libres de modificaciones no autorizadas, una amenaza a la integridad de la información de los datos de una organización es un cambio no autorizado a los datos almacenados en un recurso de red o en tránsito entre los recursos[2].

Artero (2008), la Seguridad de la Información abarca la protección tanto de los Sistemas de Información como de las Redes y de los Computadores. Se trata de un continuo desafío, ya que más que un problema tecnológico, constituye hoy en día un elemento clave que posibilita los negocios y permite que las organizaciones puedan llevar a cabo sus objetivos corporativos[3].

La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

[2] KIM & SOLOMON, David, Michael G, Fundamentals of information systems security, Jones and Bartlett learning, 1st edition, 2010.
[3] ARTERO, J.L, Seguridad en la Información, S.A. Ediciones Paraninfo, 2008.

FIGURA 2. CARACTERÍSTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

Fuente:http://iberplanet.com/es/wpcontent/uploads/2015/02/caracteristicasISO27001.png

Adicionalmente, deben considerarse los conceptos de:

- **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución.

Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

- **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- **Confiabilidad de la Información:** la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

- **Información:** se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- **Sistema de Información:** se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- **Tecnología de la Información:** se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Estos conceptos permiten desde el proceso de auditoría en la empresa Expreso Juanambú garantizar que la seguridad de la información va ser analizada en todos los aspectos mencionados, para así poder crear un buen trabajo de auditoría.

Una vez abordados estos conceptos de seguridad de la información es fundamental la gestión de la seguridad como elemento administrativo en la empresa Expreso Juanambú para así poder garantizar la seguridad de sus recursos.

1.3.2. Administración de seguridad. Newman (2009), la Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada. Esta es una de las principales preocupaciones de una empresa, proteger su información[4].

Cano & Jeimy (2013), Asegurar la información clave en el contexto empresarial, en un mundo altamente interconectado, basado en redes sociales y con sobrecarga de información (particularmente instantánea), es un reto para cualquier ejecutivo de seguridad de la información. En este sentido, entender la dinámica corporativa y la forma como la inseguridad de la información se materializa es una competencia estratégica que los responsables de la seguridad de la información deben desarrollar para mantenerse alertas y anticiparse a los movimientos de la inevitabilidad de la falla[5].

Las buenas prácticas de administración indican que el establecimiento claro de la misión de una organización es indispensable para que todos los funcionarios ubiquen sus propios esfuerzos y los direccionen en bien de la misma. Además, permite elaborar políticas operativas que facilitan el cumplimiento de la misión de la organización, que pueden entenderse como reglas que hay que seguir obligatoriamente.

Es usual que la alta gerencia cometa errores en cuanto a la seguridad de la información de sus organizaciones, como por ejemplo suponer que los problemas desaparecen si se ignoran, no entender cuánto dinero vale su información y que tanto depende la organización de ella, no lidiar con los aspectos operacionales de la seguridad, no entender la relación que existe entre la seguridad y los problemas

[4] NEWMAN, Robert C, Computer Security protecting digital resources. Jones and Bartlett publishers, 2010.
[5] CANO, M; JEIMY, J. Inseguridad de la Información, S.A. Marcombo, Barcelona, 2013.

de funcionamiento y marcha de la organización, entre otros. Si la administración empresarial propone una misión para direccionar estratégicamente la organización, es posible hacer una analogía con la "administración de la seguridad", y es posible entonces ejecutar una "Misión de Seguridad", que "solucione las falencias, ubicando la seguridad informática al mismo nivel que otras actividades sustantivas de la organización, elaborando un plan de seguridad informática clara, promulgando políticas que se derivan de dicha misión y determinando qué mecanismos se requieren para implementar esas políticas"[6].

FIGURA 3. CICLO DE LA IMPLEMENTACIÓN DE LA ADMINISTRACIÓN EN SEGURIDAD

Fuente:https://www.microsoft.com/spain/technet/recursos/articulos/images/rmch0301_big.gif

Una buena administración de seguridad en la empresa Expreso Juanambú, permitirá que la empresa empiece a organizar su información y a dar importancia a sus datos e información.

[6] DALTABUIT GODÁS, Enrique, VÁZQUEZ, José de Jesús, La Seguridad de la Información. Limusa Noriega Editores, México, 2007. Pág. 215.

Para poder realizar una buena administración de seguridad es necesario empezar a realizar el proceso de auditoría en la empresa Expreso Juanambú, por esta razón se quiere abordar el concepto de auditoría de seguridad de sistemas de información.

1.3.3. Auditoría de seguridad de sistemas de información. Piattini (2008), en la actualidad nadie duda que la información se ha convertido en uno de los activos principales de las empresas, representando las tecnologías y los sistemas relacionados con la información su principal ventaja estratégica. Las organizaciones invierten enormes cantidades de dinero y tiempo en la creación de sistemas de información y en la adquisición y desarrollo de tecnologías que les ofrezcan la mayor productividad y calidad posibles. Es por eso que los temas relativos a la auditoría de las tecnologías y los sistemas de información (TSI) cobran cada vez más relevancia a nivel mundial[7].

El sistema de información se refiere al almacenamiento, proceso, comunicación, entrada y salida de la información. “Sobre estas funciones elementales y a través del sistema operativo y las aplicaciones, se mantiene la información, se envían los mensajes y se ofrecen los servicios con valor para la organización”[8].

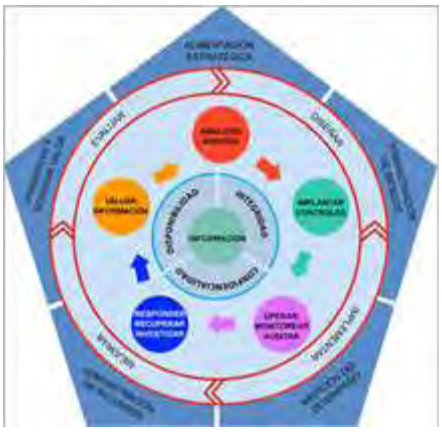
Para ello, se establece un SGSI (Sistema de Gestión de la Seguridad de la Información), que es aquella parte del sistema general de gestión que comprende los recursos necesarios para implantar la gestión de la seguridad de la información en una organización[9].

[7] PIATTINI VELTHUIS, Mario, Auditoría de Tecnologías y Sistemas de Información, Ra-Ma Editores, Madrid, 2008.
[8] ACEITUNO CANAL, Vicente “Seguridad de la Información: expectativas, riesgos y técnicas de protección” Op.Ed Noriega Editores. México. D.F. 2006
[9] GÓMEZ VIEITES, Álvaro. 2007, Enciclopedia de la Seguridad Informática, Alfa omega Grupo editor, México, Primera Edición, Pág. 18.

Una auditoría de seguridad informática o auditoría de seguridad de sistemas de información (SI) es el estudio que comprende el análisis y gestión de sistemas, llevado a cabo por profesionales para identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables, quienes deberán establecer medidas preventivas de refuerzo y/o corrección siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

FIGURA 4. AUDITORÍA DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN



Fuente: http://www.all4sec.es/wp-content/uploads/2011/09/servicios-consultoria-de-seguridad.png

Las auditorías de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad[10].

1.3.3.1. Fases de una auditoría. Los servicios de auditoría constan de las siguientes fases:

- Enumeración de redes, topologías y protocolos
- Verificación del cumplimiento de los estándares internacionales. ISO, COBIT, etc.
- Identificación de los sistemas operativos instalados
- Análisis de servicios y aplicaciones
- Detección, comprobación y evaluación de vulnerabilidades
- Medidas específicas de corrección
- Recomendaciones sobre implantación de medidas preventivas

1.3.3.2. Tipos de auditoría. Los servicios de auditoría pueden ser de distinta índole:

Auditoría de seguridad interna. En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno.

Auditoría de seguridad perimetral. En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores.

[10] AUDITORÍA DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN**.** [En línea] Disponible en internet. http://es.wikipedia.org/wiki/Auditor%C3%ADa_de_seguridad_de_sistemas_de_informaci%C3%B3n[Citado diciembre de 2014].

Test de intrusión. El test de intrusión es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada. Es un complemento fundamental para la auditoría perimetral.

Análisis forense. El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperatividad del sistema, el análisis se denomina análisis post-mortem.

Auditoría de páginas web. Entendida como el análisis externo de la web, comprobando vulnerabilidades como la inyección de código SQL, Verificación de existencia y anulación de posibilidades de Cross Site Scripting (XSS), etc.

Auditoría de código de aplicaciones. Análisis del código tanto de aplicaciones páginas Web como de cualquier tipo de aplicación, independientemente del lenguaje empleado.

Realizar auditorías con cierta frecuencia asegura la integridad de los controles de seguridad aplicados a los sistemas de información. Acciones como el constante cambio en las configuraciones, la instalación de parches, actualización de software y la adquisición de nuevo hardware hacen necesario que los sistemas estén continuamente verificados mediante auditoría.

1.3.3.3. Estándares de auditoría informática y de seguridad. Una auditoría se realiza con base a un patrón o conjunto de directrices o buenas prácticas sugeridas. Existen estándares orientados a servir como base para auditorías de informática. Uno de ellos es COBIT (Objetivos de Control de la Tecnologías de la Información), dentro de los objetivos definidos como parámetro, se encuentra el "Garantizar la Seguridad de los Sistemas". Adicional a este estándar podemos encontrar el

estándar ISO 27002, el cual se conforma como un código internacional de buenas prácticas de seguridad de la información, este puede constituirse como una directriz de auditoría apoyándose de otros estándares de seguridad de la información que definen los requisitos de auditoría y sistemas de gestión de seguridad, como lo es el estándar ISO 27001.

1.3.3.4. Serie de normas 27000. A semejanza de otras normas ISO, ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Algunas de las normas que conforman la serie 27000 van orientadas precisamente a documentar mejores prácticas en aspectos o incluso cláusulas concretas de la norma ISO/IEC 27001 de modo que se evite reinventar la rueda con el sustancial ahorro de tiempo en la implantación[11].

- **ISO/IEC 27000:** publicada el 1 de mayo de 2009, revisada con una segunda edición de 01 de diciembre de 2012 y una tercera edición de 14 de enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para

[11] EL PORTAL DE ISO 27001 EN ESPAÑOL. [en línea] Disponible en internet. http://www.iso27000.es/iso27000.html [citado diciembre de 2014].

evitar convertirlo en el único marco de referencia para la mejora continua). Existen versiones traducidas al español, aunque hay que prestar atención a la versión descargada.

- **ISO/IEC 27001:** publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI, a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Desde el 28 de noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007 y puede adquirirse online en AENOR (también en lengua gallega). En 2009, se publicó un documento adicional de modificaciones (UNE-ISO/IEC 27001:2007/1M: 2009). Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27001), Venezuela (Fondonorma ISO/IEC 27001), Argentina (IRAM-ISO IEC 27001), Chile (NCh-ISO27001), México (NMX-I-041/02-NYCE) o Uruguay (UNIT-ISO/IEC 27001). El original en inglés y la traducción al francés pueden adquirirse en iso.org.

- **ISO/IEC 27002:** desde el 1 de julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. Publicada en España como UNE-ISO/IEC 27002:2009 desde

el 9 de diciembre de 2009 (a la venta en AENOR). Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27002), Venezuela (Fondonorma ISO/IEC 27002), Argentina (IRAM-ISO-IEC 27002), Chile (NCh-ISO27002), Uruguay (UNIT-ISO/IEC 27002) o Perú (como ISO 17799; descarga gratuita).

- **ISO/IEC 27003:** publicada el 01 de febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación. En España, esta norma aún no está traducida, pero sí en Uruguay (UNIT-ISO/IEC 27003).

- **ISO/IEC 27004:** publicada el 15 de diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001. En España, esta norma aún no está traducida, sin embargo, sí lo está en Argentina (IRAM-ISO-IEC 27004) o Uruguay (UNIT-ISO/IEC 27004).

- **ISO/IEC 27005:** publicada en segunda edición el 1 de junio de 2011 (primera edición del 15 de junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Su primera publicación revisó y retiró las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000. En España, esta norma no está

traducida, sin embargo, sí lo está, para la versión de 2008, en países como México (NMX-I-041/05-NYCE), Chile (NCh-ISO27005), Uruguay (UNIT-ISO/IEC 27005) o Colombia (NTC-ISO-IEC 27005).

- **ISO/IEC 27006:** publicada en segunda edición el 1 de diciembre de 2011 (primera edición del 1 de marzo de 2007). Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001:2005 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma. El original en inglés puede adquirirse en iso.org. En España, esta norma no está traducida, sin embargo, sí lo está, para la versión de 2007, en México (NMX-I-041/06-NYCE) o Chile (NCh-ISO27001). Actualmente ha iniciado un nuevo periodo de revisión para una nueva versión 3.

- **ISO/IEC 27007:** publicada el 14 de noviembre de 2011. No certificable. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011. En España, esta norma no está traducida.

1.3.3.5. COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas). 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. El COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva de negocios.

Las siglas COBIT significan Objetivos de Control para Tecnología de Información y Tecnologías relacionadas (Control Objectives for Information Systems and related Technology). El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (Information Systems Audit and Control Association).

COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de tecnología. Vinculando tecnología informática y prácticas de control, el modelo COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

- **MISIÓN DEL COBIT**

Buscar, desarrollar, publicar y promover un autoritario y actualizado conjunto internacional de objetivos de control de tecnologías de la información, generalmente aceptadas, para el uso diario por parte de gestores de negocio y auditores.

- **BENEFICIOS COBIT**

- ✓ Mejor alineación basada en una focalización sobre el negocio.
- ✓ Visión comprensible de TI para su administración.
- ✓ Clara definición de propiedad y responsabilidades.
- ✓ Aceptabilidad general con terceros y entes reguladores.

- ✓ Entendimiento compartido entre todos los interesados basados en un lenguaje común.
- ✓ Cumplimiento global de los requerimientos de TI planteados en el Marco de Control Interno de Negocio COSO.

- **ESTRUCTURA**

La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

La adecuada implementación de un modelo COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado.

- **DOMINIOS COBIT**

El conjunto de lineamientos y estándares internacionales conocidos como COBIT, define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro "dominios" principales, a saber:

FIGURA 5. DOMINIOS COBIT

Fuente:http://1.bp.blogspot.com/A7bz95P4sL8/T5dEp6HSVlI/AAAAAAAAAB0/XQ377ObKvKo/s1600/figura2.png

PLANIFICACIÓN Y ORGANIZACIÓN: este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

ADQUISICIÓN E IMPLANTACIÓN: para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

SOPORTE Y SERVICIOS: en este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

MONITOREO: todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda. Estos dominios y objetivos de control facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

- **USUARIOS**

La Gerencia: para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.

Los Usuarios finales: quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.

Los Auditores: para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.

Los Responsables de TI: para identificar los controles que requieren en sus áreas.

También, puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de la TI en las empresas.

Características

- 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).

PRINCIPIOS:

El enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con las TI que deben ser administrados por procesos de TI.

Requerimientos de la información del negocio: para alcanzar los requerimientos de negocio, la información necesita satisfacer ciertos CRITERIOS:

Requerimientos de calidad: calidad, costo y entrega.

Requerimientos fiduciarios: efectividad y eficiencia operacional, confiabilidad de los reportes financieros y cumplimiento le leyes y regulaciones.

Requerimientos de seguridad: confidencialidad, integridad y disponibilidad.

- **NIVELES COBIT**

Se divide en 3 niveles, los cuales son los siguientes:

Dominios: agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.

Procesos: conjuntos o series de actividades unidas con delimitación o cortes de control.

Actividades: acciones requeridas para lograr un resultado medible.

COMPONENTES COBIT

Resumen ejecutivo: es un documento dirigido a la alta gerencia presentando los antecedentes y la estructura básica de COBIT. Además, describe de manera general los procesos, los recursos y los criterios de información, los cuales conforman la "Columna Vertebral" de COBIT.

Marco de referencia (Framework): incluye la introducción contenida en el resumen ejecutivo y presenta las guías de navegación para que los lectores se orienten en la exploración del material de COBIT haciendo una presentación detallada de los 34 procesos contenidos en los cuatro dominios.

Objetivos de control: integran en su contenido lo expuesto tanto en el resumen ejecutivo como en el marco de referencia y presenta los objetivos de control detallados para cada uno de los 34 procesos[12].

[12] COBIT (OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS). [en línea] Disponible en internet. http://www.monografias.com/trabajos93/cobit-objetivo-contro-tecnologia-informacion-y-relacionadas/cobit-objetivo-contro-tecnologia-informacion-y-relacionadas.shtml [citado diciembre de 2014].

PLANEAR Y ORGANIZAR

- PO1 Definir el plan estratégico de TI.
- PO2 Definir la arquitectura de la información
- PO3 Determinar la dirección tecnológica.
- PO4 Definir procesos, organización y relaciones de TI.
- PO5 Administrar la inversión en TI.
- PO6 Comunicar las aspiraciones y la dirección de la gerencia.
- PO7 Administrar recursos humanos de TI.
- PO8 Administrar calidad.
- PO9 Evaluar y administrar riesgos de TI
- PO10 Administrar proyectos.
- PO11 Administración de Calidad

ADQUIRIR E IMPLANTAR

- AI1 Identificar soluciones automatizadas.
- AI2 Adquirir y mantener el software aplicativo.
- AI3 Adquirir y mantener la infraestructura tecnológica
- AI4 Facilitar la operación y el uso.
- AI5 Adquirir recursos de TI.
- AI6 Administrar cambios.

MONITOREAR Y EVALUAR

- ME1 Monitorear y evaluar el desempeño de TI.
- ME2 Monitorear y evaluar el control interno
- ME3 Garantizar cumplimiento regulatorio.
- ME4 Proporcionar gobierno de TI.

PRESTACIÓN Y SOPORTE

- DS1 Definir y administrar niveles de servicio.
- DS2 Administrar servicios de terceros.
- DS3 Administrar desempeño y capacidad.
- DS4 Garantizar la continuidad del servicio.
- DS5 Garantizar la seguridad de los sistemas.
- DS6 Identificar y asignar costos.
- DS7 Educar y entrenar a los usuarios.
- DS8 Administrar la mesa de servicio y los incidentes.
- DS9 Administrar la configuración.
- DS10 Administrar los problemas.
- DS11 Administrar los datos.
- DS12 Administrar el ambiente físico.
- DS13 Administrar las operaciones.

Tener una idea clara de estos conceptos y saber cuáles son los estándares de auditoría que se van a aplicar beneficia a la empresa Expreso Juanambú y facilita el trabajo de auditoría.

Para poder realizar una auditoría aplicando dos estándares de auditoría en este caso ISO 27000 Y COBIT se debe conocer cómo aplicar y cómo usar estos estándares en el proceso de auditoría.

1.3.4. Alineando cobit® 4.1 e iso/iec 27002 en beneficio de la empresa

1.3.4.1. Resumen ejecutivo. Cada empresa necesita ajustar la utilización de estándares y prácticas a sus requerimientos individuales. En este sentido, los dos estándares/prácticas cubiertos en esta guía pueden desempeñar un papel muy útil, COBIT® e ISO/IEC 27002 para ayudar a definir lo que debería hacerse.

La creciente adopción de mejores prácticas de TI se explica porque la industria de TI requiere mejorar la administración de la calidad y la confiabilidad de TI en los negocios y para responder a un creciente número de requerimientos regulatorios y contractuales.

Sin embargo, existe el peligro que las implementaciones de estas mejores prácticas, potencialmente útiles, puedan ser costosas y desenfocadas si son tratadas como guías puramente técnicas. Para ser más efectivos, las mejores prácticas deberían ser aplicadas en el contexto del negocio, enfocándose donde su utilización proporcione el mayor beneficio a la organización. La alta dirección, los gerentes, auditores, oficiales de cumplimiento y directores de TI, deberían trabajar en armonía para estar seguros que las mejores prácticas conduzcan a servicios de TI económicos y bien controlados.

Las mejores prácticas de TI posibilitan y soportan:

- Una mejor gestión de TI, lo que es crítico para el éxito de la estrategia de la empresa.
- Un gobierno eficaz de las actividades de TI.
- Un marco de referencia eficaz para la gestión de políticas, controles internos y prácticas definidas, lo que es necesario para que todos sepan lo que hay que hacer.

- Muchos otros beneficios, incluyendo ganancia de eficiencias, menor dependencia de expertos, menos errores, mejora de la confianza de los socios de negocios y de reguladores.

Este documento aplica en general a todas las mejores prácticas de TI, pero se enfoca en tres prácticas y estándares específicos, los que están siendo ampliamente adoptados a nivel global y que han sido actualizadas para incorporar las últimas versiones:

- COBIT ® 4.1: publicado por el ITGI y posicionado como un marco de referencia de alto nivel para el control y el gobierno de TI.
- ISO/IEC 27002:2005: publicado por ISO (International Organization for Standardization) y por IEC (International Electrotechnical Commission), derivado de la norma BS 7799 del gobierno británico, renombrada ISO/IEC 17799:2005, para proporcionar un marco de referencia del estándar para gestión de seguridad de información.

La implementación de las mejores prácticas debería ser consistente con el marco de control y la gestión de riesgos de la empresa, apropiada para la empresa e integrada con otras metodologías y prácticas que estén siendo utilizadas. Los estándares y las mejores prácticas no son una panacea; su efectividad depende de cómo se implementan y mantienen. Estas son mucho más útiles cuando son aplicadas como un bloque de principios y como un punto de partida para adaptar procedimientos específicos. Para evitar prácticas que nunca se pongan en ejecución (‘shelfware’), la dirección y el staff deben entender lo que hay que hacer, cómo hacerlo y porqué es importante hacerlo.

La implementación debe ser adaptada a la empresa, priorizada y planificada para lograr su uso eficaz.

Para lograr el alineamiento de las mejores prácticas con los requerimientos del negocio, se deberían utilizar procesos formales que soporten el buen gobierno de TI. La OGC proporciona guías de gestión a través de sus herramientas Successful Delivery Toolkit (www.ogc.gov.uk/sdtoolkit/), PRINCE2 como marco de referencia de las mejores prácticas para gestión de proyectos, Managing Successful Programmes (MSP) y Management of Risk (M_o_R®): Guidance for Practitioners para gestión de riesgos (ver www.bestmanagement-practice.com/). El ITGI proporciona IT Governance Implementation Guide Using COBIT and Val IT, 2nd Edition.

COBIT puede ser utilizado en los más altos niveles de gobierno de TI, proporcionando un marco de referencia global de control basado en el modelo de procesos de TI que el ITGI pretende se pueda adaptar a cada empresa. También hay una necesidad de procesos detallados y estandarizados para profesionales.

Prácticas específicas y estándares como ISO/IEC 27002, cubren áreas específicas y pueden ser mapeadas al marco de referencia COBIT, proporcionando así una jerarquía de materiales de orientación.

1.3.4.2. ¿Cuál de la mejor forma de implementar COBIT, e ISO/IEC 27002?. No hay duda que las políticas y procedimientos de gestión eficaces ayudan a asegurar que TI se gestione como un componente más de las actividades cotidianas. La adopción de estándares y mejores prácticas facilita la rápida aplicación de buenos procedimientos y evita retrasos en la creación innecesaria de nuevos enfoques en los que hay que ponerse de acuerdo. Sin embargo, las mejores prácticas adoptadas han de ser compatibles con un marco de gestión de riesgos y de control apropiado para la organización, debiendo integrarse con otros métodos y prácticas que se estén utilizando. Los estándares y las mejores prácticas no son una panacea; su efectividad depende de cómo se implementen y se mantengan actualizados. Son

muy útiles cuando se aplica como un conjunto de principios y como punto de partida para la adaptación de procedimientos más específicos.

Para asegurar que las políticas y los procedimientos se utilizan con eficacia, se requiere un cambio de manera que la administración y el personal entiendan qué hacer, cómo hacerlo y por qué es importante.

Para que las mejores prácticas sean eficaces, es mejor utilizar un lenguaje común y un enfoque estándar orientado hacia las necesidades reales del negocio, ya que garantiza que todos sigan el mismo conjunto de objetivos, asuntos y prioridades.

- **Elaboración**

Todas las empresas necesitan adaptar el uso de estándares y prácticas tales como los presentados en este documento, para ajustar sus requisitos individuales. Los documentos de guía pueden desempeñar un papel muy útil. COBIT e ISO/IEC 27002 para ayudar a definir qué debería hacerse. Las aplicaciones típicas para este tipo de estándares y prácticas son las siguientes:

Para apoyar la gobernabilidad a través de:

- ✓ Proporcionar una política de gestión y un marco de control.
- ✓ Facilitar el proceso de asignación de propietarios, responsabilidades claras y rendición de cuentas para las actividades de TI.
- ✓ Alinear los objetivos de TI con los objetivos del negocio, definiendo prioridades y la asignación de recursos.
- ✓ Asegurar el retorno de la inversión y optimizar los costos.
- ✓ Asegurar la identificación de los riesgos significativos y que sean transparentes para la administración, que se asigna la responsabilidad en la gestión del riesgo

y se integre en la organización, y asegurando a la dirección que se han implementado controles eficaces.

- ✓ Asegurar que los recursos se han organizado de manera eficiente y que existe suficiente capacidad (infraestructura técnica, procesos y habilidades) para ejecutar la estrategia de TI.
- ✓ Asegurar que las actividades críticas de TI pueden ser monitoreadas y medidas, de modo que los problemas puedan ser identificados y que las medidas correctivas puedan ser adoptadas.

Para definir los requisitos del servicio y las definiciones del proyecto, tanto internamente como con los proveedores de servicios, por ejemplo:

- ✓ Estableciendo objetivos claros de TI relacionados al negocio, así como métricas.
- ✓ Definiendo los servicios y proyectos en términos de usuario final.
- ✓ Elaborando acuerdos de niveles de servicio y contratos que pueden ser monitoreados por los clientes.
- ✓ Asegurando que los requisitos del cliente han sido plasmados apropiadamente en requisitos operativos y técnicos de TI.
- ✓ Considerando los portafolios de servicios y de proyectos en conjunto, a fin de establecer las prioridades relativas, de modo que los recursos se asignen de manera equitativa y viable.

Para verificar la capacidad profesional o demostrar competencia en el mercado a través de:

- ✓ Las evaluaciones y las auditorías independientes de terceros.
- ✓ Compromisos contractuales.
- ✓ Constancias y certificaciones.

Para facilitar la mejora continua por:

- ✓ Evaluaciones de madurez.
- ✓ Análisis de brechas.
- ✓ Benchmarking.
- ✓ Planificación de la mejora.
- ✓ Evitar la reinvención de buenos enfoques ya probados.

Como marco para la auditoría, evaluación y una visión externa a través de:

- ✓ Criterios objetivos y mutuamente entendidos.
- ✓ Benchmarking para justificar las debilidades y brechas en los controles.
- ✓ Incrementando la profundidad y el valor de las recomendaciones mediante enfoques generalmente aceptados.

- **Priorización**

Para evitar implementaciones de estándares y mejores prácticas costosas y fuera de foco, las empresas necesitan priorizar dónde y cómo utilizarlos. La empresa necesita un plan de acción eficaz que se adapte a sus circunstancias y necesidades particulares. En primer lugar, es importante que la Alta Dirección asuma el liderazgo del gobierno de TI y establezca la dirección que la gestión debe seguir. La Alta Dirección debería:

- ✓ Asegurarse que TI está en la agenda.
- ✓ Cuestionar las actividades de gestión en materia de TI para asegurar que los problemas de TI son revelados.
- ✓ Guiar a la administración ayudando a alinear las iniciativas de TI con las necesidades reales del negocio. Asegurar que la administración valora el impacto potencial de los riesgos de TI en el negocio.

- ✓ Insistir en que el desempeño de TI sea medido y se comunique a la Alta Dirección.
- ✓ Establecer un comité de dirección de TI o consejo de gobierno de TI con la responsabilidad de comunicar los aspectos de TI a la Alta Dirección y la administración.
- ✓ Insistir en que exista un marco de gestión para el gobierno de TI basada en un enfoque común (por ejemplo, COBIT) y un marco de mejores prácticas para la gestión de servicios TI y seguridad basadas en un estándar global y de facto (por ejemplo, ITIL e ISO/IEC 27002).

- **Planificación**

Con el mandato y la dirección en marcha, la administración puede poner en práctica un enfoque de implementación. Para ayudar a que la administración decida dónde empezar y asegurar que el proceso de implementación ofrece resultados positivos en donde más se necesitan, se sugieren los siguientes pasos, basados en la guía IT Governance Implementation Guide del ITGI:

1. Establecer un marco organizativo (idealmente como parte de una iniciativa global de gobierno de TI), con objetivos y responsabilidades claras, la participación de todas las partes involucradas, quienes impulsarán la implementación y la asumirán como una iniciativa propia.
2. Alinear la estrategia de TI con los objetivos del negocio. ¿En cuáles de los objetivos de negocio actuales, TI tiene una contribución significativa? Obtener una buena comprensión del entorno empresarial, el apetito de riesgo, la estrategia del negocio, y su relación con TI. Las directrices de gestión de COBIT (específicamente los objetivos y las métricas), ayudan a definir los objetivos de TI. Utilizada en conjunto con ITIL, los servicios y los acuerdos de niveles de servicios (ANS) se puede definir en términos de usuario final.

3. Entender y definir los riesgos. Dados los objetivos de negocio, ¿cuáles son los riesgos relativos a la capacidad de TI para cumplirlos? Considerar lo siguiente:

- Antecedentes y patrones de desempeño.
- Factores organizacionales actuales de TI.
- La complejidad y el tamaño/alcance de la infraestructura de TI existente o prevista.
- Las vulnerabilidades inherentes de la infraestructura de TI existente o prevista.

La naturaleza de las iniciativas de TI que están siendo consideradas, por ejemplo: nuevos proyectos de sistemas, consideraciones de outsourcing, cambios en la arquitectura, etc.

El proceso de COBIT para la gestión del riesgo (PO9) y la aplicación del marco de control de COBIT y los criterios de información, ayudarán a asegurar que los riesgos se identifican y se asignan.

4. Definir las áreas objetivo y determinar las áreas de proceso de TI que son críticos para la entrega de valor y gestionar estas áreas de riesgo. El marco de procesos COBIT puede ser utilizado como la base y los objetivos de seguridad de la ISO/IEC 27002. La publicación Management of Risk: Guidance to Practitioner de la OGC también puede ser de ayuda en la evaluación y gestión de los riesgos en cualquiera de los cuatro niveles principales (estratégico, programa, proyecto u operativo).
5. Analizar la capacidad vigente e identificar las brechas. Realizar una evaluación de la capacidad de madurez para saber dónde es que más se necesitan mejoras.
6. Desarrollar estrategias de mejora y decidir cuáles son los proyectos de mayor prioridad que ayudarán a mejorar la gestión y el gobierno de estas áreas importantes. Esta decisión debe basarse en el beneficio potencial y la facilidad de implementación, enfocado en los procesos importantes de TI y en las

competencias básicas. Se deberían perfilar proyectos específicos de mejora como parte de una iniciativa de mejora continua.

7. Medir los resultados, estableciendo un mecanismo de puntuación para medir el desempeño actual y monitorear los resultados de nuevas mejoras, considerando como mínimo, las siguientes preguntas clave:

- ¿La estructura organizacional apoyará la implementación de la estrategia?
- ¿Las responsabilidades de la gestión de riesgos están integradas en la organización?
- ¿Existe infraestructura que facilite y apoye la creación y el intercambio de información comercial vital?
- ¿Se han comunicado las estrategias y los objetivos de manera efectiva a todos los que necesitan saber en la organización?

Los objetivos y las métricas de COBIT y el enfoque de mejora continua de siete pasos de ITIL pueden formar la base de un sistema de puntuación.

8. Repetir los pasos 2 a 7 con una frecuencia regular.

Evitar obstáculos.

Existen otras reglas obvias pero pragmáticas que la administración debe seguir:

- Tratar la iniciativa de implementación como una actividad de proyecto con una serie de fases en lugar de un solo esfuerzo extraordinario.
- Recordar que la implementación supone un cambio cultural, así como nuevos procesos. Por lo tanto, un factor clave de éxito es facilitar y motivar estos cambios.
- Asegurar de que haya una comprensión clara de los objetivos.

- Manejar las expectativas. En la mayoría de las empresas, lograr la supervisión exitosa de TI toma tiempo y es un proceso de mejora continua.
- Concentrar primero en las áreas donde es más fácil hacer cambios y lograr mejoras, y desde allí, construir paso a paso.
- Obtener el respaldo de la Alta Dirección. Esto necesita estar basado en los principios de la mejor gestión de las inversiones de TI7.
- Evitar las iniciativas que se perciben como un ejercicio puramente burocrático.
- Evitar listas de verificación fuera de foco.

- **Alinear las mejores prácticas**

Las mejores prácticas de TI deben ajustarse a los requisitos del negocio y ser integradas entre sí y con los procedimientos internos. COBIT puede ser utilizado en el más alto nivel, ofreciendo un marco general de control basado en un modelo de procesos de TI que debería adaptarse a cada organización. Los estándares y las prácticas específicas, tales como ISO/IEC 27002 abarcan áreas discretas y pueden ser mapeadas en el marco COBIT, estructurando una jerarquía de materiales de orientación.

Estos conceptos forman parte fundamental de este trabajo de grado ya que desde un principio la idea general fue utilizar COBIT e ISO e implantarlos en la empresa Expreso Juanambú y así poder garantizar las buenas prácticas en el uso de la seguridad de la información.

Después de realizar una correcta alineación entre COBIT e ISO se debe contar con una herramienta para gestionar los riesgos y para dar un mayor peso a la investigación se utilizó MAGERIT.

1.3.5. MAGERIT. es el acrónimo de “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Publicas”, creado por el

Consejo Superior de Administración Electrónica (CSAE). El uso de esta metodología es de carácter público, pertenece al Ministerio de Administraciones Públicas (MAP) de España.

“No es posible una aplicación racional de medidas de seguridad sin antes analizar los riesgos para, así implantar las medidas proporcionadas a estos riesgos, al estado de la tecnología y a los costes (tanto de la ausencia de seguridad como de las salvaguardas)”[13].

“La Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones públicas, MAGERIT, es un método formal para investigar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos”[14].

“MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista”.

MAGERIT persigue los siguientes objetivos:

[13] PAREDES FIERRO, Geomayra Alexandra, VEGA NOBOA, Mayra Alexandra, Desarrollo de una Metodología para la Auditoría de Riesgos Informáticos (físicos y lógicos) y su aplicación al Departamento de Informática de la Dirección Provincial de Pichincha del Consejo de la Judicatura”, Tesis Escuela Superior Politécnica de Chimborazo Facultad de Informática y Electrónica, Riobamba, 2011, p. 109

[14] Definición de necesidades en términos de seguridad informática, http://www.coit.es/publicac/publbit/bit128/bitcd1/legisla/pg5m21.htm

Directos:

a) Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
b) Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
c) Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos:

Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Actualmente, se encuentra en la versión 3, durante el periodo transcurrido desde la publicación de la primera versión de MAGERIT (1997), el análisis de riesgos se ha venido consolidando como paso necesario para la gestión de la seguridad.

La versión 2 y 3 de MAGERIT se ha estructurado en tres libros: “El Método”, un “Catálogo de Elementos” y una “Guía de Técnicas”.

El método: “realización del análisis y de la gestión: en la planificación del análisis y gestión de riesgos se establecen las consideraciones necesarias para arrancar el proyecto, investigando la oportunidad de realizarlo, definiendo los objetivos que ha de cumplir y el dominio (ámbito) que abarcará, planificando los medios materiales y humanos para su realización e iniciando materialmente el propio lanzamiento del proyecto”.

Análisis de riesgos: en el análisis de riesgos se identifican y valoran los elementos componentes del riesgo, obteniendo una estimación de los umbrales de riesgo deseables.

Elementos del análisis de riesgos: aquí el Analista de Riesgos es el profesional especialista que maneja seis elementos básicos:

a) Activos: el activo esencial es la información o dato.
b) Amenazas: determinar las amenazas que pueden afectar a cada activo, hay que estimar cuán vulnerable es el activo en dos sentidos: degradación: como es de perjudicial y frecuencia: cada cuanto se materializa la amenaza.

Las amenazas según MAGERIT, pueden ser de 4 tipos como se indica en la Tabla 1. Tipo de amenazas MAGERIT contenida en el ANEXO K – PLANTILLAS Y TABLAS.

c) Vulnerabilidades: potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.
d) Impacto: es el daño sobre el activo causado por la amenaza, conociendo el valor de los activos sería muy sencillo calcular el valor del impacto
e) Riesgo: es la medida de la posibilidad que existe en que se materialice una amenaza. conociendo el riesgo ya podemos calcular la frecuencia
f) Salvaguardas: es un mecanismo de protección frente a las amenazas.

Catálogo de elementos: ofrece unas pautas y elementos estándar en cuanto a: tipos de activos, dimensiones de valoración de los activos, escala de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información. Se persiguen dos objetivos:

a) Por una parte, facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.
b) Por otra, homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

Dicho catálogo está conformado por las siguientes tablas: Tabla 2. Tipos de activos, Tabla 3. Dimensiones de valoración de un activo, Tabla 4. Valoración cualitativa y Tabla 5. Valoración cuantitativa que pueden consultarse en el ANEXO K – PLANTILLAS Y TABLAS.

Muchos activos de información no son inventariables en sentido contable o como 'valor de cambio'; pero no por ello dejan de tener 'valor de uso' para la organización.

Controles: hay diferentes aspectos en los cuales puede actuar un control para alcanzar sus objetivos de limitación del impacto y/o mitigación del riesgo:

[PR] se requieren procedimientos tanto para la operación de los controles preventivos como para la gestión de incidencias y la recuperación tras las mismas.

[PER] política de personal, que es necesaria cuando se consideran sistemas atendidos por personal. La política de personal debe cubrir desde las fases de especificación del puesto de trabajo y selección, hasta la formación continua.

Guía de técnicas: ***"***proporciona algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos".

Es importante resaltar que la notación que se propone en la aplicación de la técnica en ningún caso se considerará obligatoria. Cada organización podrá utilizar la

notación que desee, la que suele utilizar o la que ofrecen sus herramientas de desarrollo, respetando las reglas y restricciones específicas de las distintas técnicas.

Técnicas específicas: se han considerado de especial interés:

a) Uso de tablas para la obtención sencilla de resultados: la experiencia ha demostrado la utilidad de métodos simples de análisis llevados a cabo por medio de tablas que, sin ser muy precisas, sí aciertan en la identificación de la importancia relativa de los diferentes activos sometidos a amenazas.

Estimación del impacto: se puede calcular el impacto con base a tablas sencillas de doble entrada. (Ver Tabla 6. Estimación del impacto en el ANEXO K – PLANTILLAS Y TABLAS).

Aquellos activos que reciban una calificación de impacto desastroso deberían ser objeto de atención inmediata.

Estimación de la probabilidad: por otra parte, se modela la probabilidad de ocurrencia de una amenaza por medio de escalas cualitativas. (Ver Tabla 7. Estimación de la probabilidad en el ANEXO K – PLANTILLAS Y TABLAS).

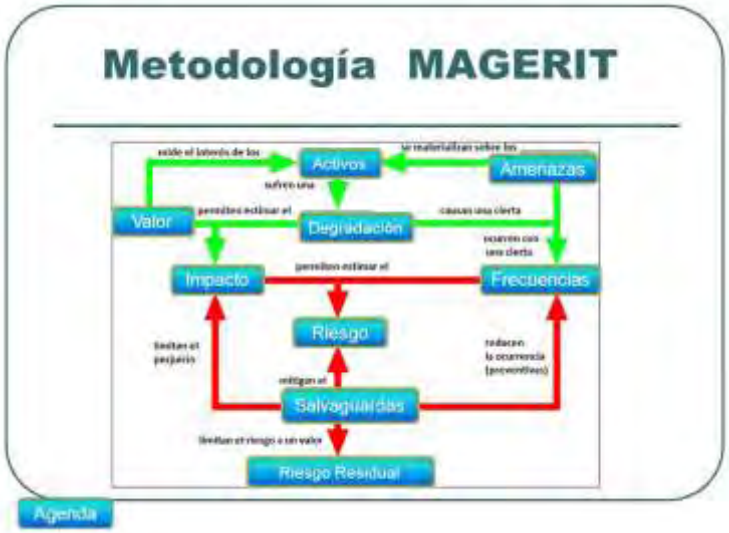
Estimación del riesgo: la estimación del riesgo es obtenida por medio de la siguiente ecuación matemática:

*Riesgo = probabilidad * impacto*

Este proceso de análisis de riesgos normalmente genera un MAPA DE RIESGOS, en el que se ubican los activos de información identificados y los cálculos realizados. (Ver Tabla 8. Mapa de riesgos en el ANEXO K – PLANTILLAS Y TABLAS).

Con los resultados obtenidos con este análisis se procede a la evaluación. Para cada activo, el proceso concluye si el riesgo es aceptable, caso contrario, se define el tratamiento (evitar, transferir o mitigar) y se establecen los controles (salvaguardas) necesarios. En esta actividad se concluye el *informe de evaluación de riesgos TI*, el cual es utilizado para elaborar el p*lan de tratamiento de riesgos*.

FIGURA 6. METODOLOGÍA MAGERIT



Fuente: http://player.slideplayer.es/6/1644740/data/images/img13.png

El objetivo general del análisis de riesgos, es identificar las causas potenciales de los principales riesgos que amenazan el entorno informático. Esta identificación se realiza en una determinada área para así tener suficiente información, optando por un diseño apropiado e implantación de mecanismos de control con el fin de minimizar los efectos de eventos no deseados.

Un minucioso análisis de riesgos; identificar, definir y revisar los controles de seguridad, determinar si se requiere incrementar las medidas de seguridad; y la

identificación de los riesgos, los perímetros de seguridad, controles de acceso y los lugares de mayor peligro, pueden hacer el mantenimiento más fácilmente.

b) Técnicas algorítmicas para la obtención de resultados elaborados: análisis de la distinción y separación de las partes de un todo hasta llegar a conocer sus principios o elementos.
c) Árboles de ataque para complementar los razonamientos de qué amenazas se ciernen sobre un sistema de información: los árboles de ataque son una técnica para modelar las diferentes formas de alcanzar un objetivo. El objetivo del atacante se usa como raíz del árbol. A partir de este objetivo, de forma iterativa e incremental se van detallando como ramas del árbol las diferentes formas de alcanzar aquel objetivo, convirtiéndose las ramas en objetivos intermedios que a su vez pueden refinarse. Los posibles ataques a un sistema se acaban modelando como un bosque de árboles de ataque.

Un árbol de ataque pasa revista a cómo se puede atacar un sistema y por tanto permite identificar qué salvaguardas se necesita desplegar para impedirlo. También permiten estudiar la actividad del atacante y por tanto lo que necesita saber y lo que necesita tener para realizar el ataque, de esta forma es posible refinar las posibilidades de que el ataque se produzca si se sabe a quién pudiera interesar el sistema y/o la información y se cruza esta información con las habilidades que se requieren.

Técnicas generales: son utilizadas en el desarrollo de un proyecto de análisis y gestión de riesgos. Se han considerado de especial interés:

a) Técnicas gráficas: histogramas, diagramas de Pareto y de tarta:

- **Por puntos y líneas:** es la forma más clásica de presentación de resultados. Se limita a usar los ejes cartesianos usando las abscisas para recoger los datos y las ordenadas para mostrar su valor.
- **Por barras:** los diagramas de barras disponen los elementos en unas coordenadas cartesianas convencionales: los elementos a considerar en un eje y los valores en el otro eje.
- **Gráficos de 'radar':** estos gráficos representan las distintas variables o factores del fenómeno en estudio sobre ejes o radios que parten de un centro. Estos radios, tantos como factores, se gradúan para representar sus niveles y posibles umbrales en escala normal o logarítmica, según convenga.
- **Diagramas de Pareto:** una gráfica de Pareto es utilizada para separar gráficamente los aspectos más significativos de un problema que el equipo sepa dónde dirigir sus esfuerzos para mejorar. Reducir los problemas más significativos (las barras más largas en una gráfica Pareto) servirá más para una mejora general que reducir los más pequeños.
- **Diagramas de tarta:** estos diagramas presentan los datos como fracciones de un círculo, distribuidos los 360º de éste en proporción al valor que es representado en cada sección. La proporción suele ser lineal; rara vez logarítmica.

b) Sesiones de trabajo: entrevistas, reuniones y presentaciones:

- **Entrevistas:** las entrevistas son reuniones con una persona o un grupo de personas con el objetivo de obtener cierta información. Las entrevistas se dicen estructuradas cuando se atiene a una serie de preguntas planificadas sin margen para la improvisación. Las entrevistas se dicen libres cuando, existiendo un objetivo claro, no existe un formulario rígido.
- **Reuniones:** las reuniones tienen como objetivo obtener información que se encuentra repartida entre varias personas, tomar decisiones estratégicas, tácticas u operativas, transmitir ideas sobre un determinado tema, analizar

nuevas necesidades de información, así como comunicar los resultados obtenidos como consecuencia de un estudio.

- **Presentaciones:** el objetivo de las presentaciones es la comunicación de avances, conclusiones y resultados por parte del equipo de trabajo al auditorio que corresponda. Se llevan a cabo con el fin de informar sobre el estado de un proyecto en su totalidad o de alguno de los procesos, o exponer uno o varios productos finales de un proceso para su aprobación.

c) Valoraciones Delphi: la técnica Delphi es un instrumento de uso múltiple adecuada para MAGERIT que se utiliza con muy variados objetivos: identificar problemas, desarrollar estrategias para la solución de problemas, fijando un rango de alternativas posibles, identificar factores de resistencia en el proceso de cambio, establecer previsiones de futuro sobre la evolución de las tendencias que se observan en un determinado campo o sector y contrastar opiniones en un tema abarcando un amplio campo de disciplinas o sectores.

Utilizar la metodología MAGERIT le da un soporte al trabajo de grado ya que es una herramienta fundamental a la hora de analizar los riesgos en una empresa.

1.4. MARCO CONCEPTUAL

Enseguida se especifican algunos términos que serán citados y utilizados en el desarrollo del proyecto.

Activos de información: los activos de información son todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede

contener importante información como lo puede ser Bases de Datos con usuarios, contraseñas, números de cuentas, etc[15].

Vulnerabilidad: es una situación inherente a los activos, o presente en su entorno, que facilita la materialización de las amenazas y las llevan a la condición de debilidad. Las vulnerabilidades son de diversos tipos como por ejemplo: la falta de conocimiento de un usuario, la transmisión a través de redes públicas, entre otras[16].

Amenaza: es aquella situación que puede ocasionar resultados negativos en las operaciones cotidianas de la empresa, generalmente se referencia como amenazas a las fallas, a los ingresos no autorizados, a los virus, a los desastres ocasionados por fenómenos físicos o ambientales, entre otros. Las amenazas logran ser de carácter físico como una inundación, o lógico como un acceso no autorizado a la base de datos[17].

Riesgo: es aquel suceso que dificulta el cumplimiento de un objetivo de manera cuantitativa. Se puede considerar como una medida de las posibilidades de incumplimiento o exceso del objetivo planteado. Así definido, un riesgo conlleva a dos tipos de consecuencias: ganancias o pérdidas. Así mismo, el riesgo se plantea solamente como amenaza determinando el grado de exposición o el grado de una pérdida (por ejemplo el riesgo de que se pierdan los datos por el daño del disco duro, virus informáticos, entre otros).

---

[15] ADMINISTRACIÓN DE REDES DE COMPUTADORES - ¿QUÉ ES UN ACTIVO DE INFORMACIÓN? [en línea] Disponible en internet. https://camiloangel.wordpress.com/2010/09/03/%C2%BFque-es-un-activo-de-informacion. [citado septiembre de 2010].

[16] METODOLOGÍA DE ANÁLISIS DE RIESGO DE LA EMPRESA LA CASA DE LAS BATERÍAS S.A DE C.V. [en línea] Disponible en internet. http://upload.wikimedia.org/wikipedia/commons/8/87/Riesgoinformatico.pdf. [citado junio de 2014].

[17] EL PORTAL DE ISO 27001 EN ESPAÑOL - GLOSARIO. [en línea] Disponible en internet. http://www.iso27000.es/glosario.html. [citado junio de 2014].

La organización Internacional para la normalización (ISO), define riesgo tecnológico, como:

“La probabilidad de que una amenaza se materialice, utilizando una vulnerabilidad existente de un activo o un grupo de activos, generándole pérdidas o daños”[18].

Impacto: es la consecuencia de la ocurrencia de las distintas amenazas y los daños por pérdidas que éstas puedan causar. Las pérdidas generadas pueden ser financieras, económicas, tecnológicas, físicas, entre otras[19].

Análisis de riesgos: es un instrumento de diagnóstico que permite establecer la exposición real a los riesgos por parte de una organización. Este análisis tiene como objetivos la identificación de los riesgos mediante la identificación de sus elementos, lograr establecer el riesgo total y consecutivamente el riesgo residual luego de aplicadas las contramedidas en términos cuantitativos o cualitativos[20].

Probabilidad: para establecer la probabilidad de ocurrencia se puede hacerlo cualitativa o cuantitativamente, considerando lógicamente, que la medida no debe contemplar la existencia de ninguna acción de control, o sea, que debe considerarse en cada caso que las posibilidades existen, que la amenaza se presenta independientemente del hecho que sea o no contrarrestada[21].

Evaluación de riesgos: este proceso incluye la medición del potencial de las pérdidas y la probabilidad de la pérdida, categorizando el orden de las prioridades[22].

[18] EL PORTAL DE ISO 27001 EN ESPAÑOL - GLOSARIO. [en línea] Disponible en internet. http://www.iso27000.es/glosario.html. [citado junio de 2014].
[19] Ibíd.
[20] Ibíd.
[21] Ibíd.
[22] Ibíd.

Objetivos de control y riesgos: los riesgos incluyen fraudes, errores, interrupción del negocio, y el uso ineficiente e inefectivo de los recursos. Los objetivos de control reducen estos riesgos y aseguran la integridad de la información, la seguridad, y el cumplimiento. La integridad de la información es resguardada por los controles de calidad del input, procesamiento, output y software[23].

1.5. MARCO LEGAL

Las instituciones tienen que tener en cuenta los aspectos legales para el apoyo de la formulación de un proyecto, es por esto que esta investigación se apoya desde lo legal en las siguientes leyes, decretos y reglamentos:

LEY ESTATUTARIA 1581 DE 2012: "Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional" [24].

DECRETO 1377 DE 2013: "Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012"[25].

Se tuvo en cuenta esta Ley a la hora de saber cuál es el respeto a las condiciones de seguridad y privacidad de la información.

LEY 1273 DEL 5 DE ENERO DE 2009: "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la

[23] COMPARACIÓN DE CONTROLES INTERNOS: COBIT, SAC Y COSO. [en línea] Disponible en internet. http://www.netconsul.com/riesgos/cci.pdf. [citado junio de 2014.
[24] LEY ESTATUTARIA 1581 DE 2012. [en línea] Disponible en internet. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. [citado mayo de 2014].
[25] DECRETO 1377 DE 2013. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646. [citado mayo de 2014].

información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones" [26].

Esta Ley habla de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, tiene una serie de artículos los cuales hablan de delitos informáticos y permitió conocer algunas infracciones a sistemas de información.

LEY 603 DE 2000: "Esta Ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales" [27].

Esta Ley obliga a las empresas a presentar un informe del tipo de software que usa la compañía, con el fin de proteger la propiedad intelectual y evitar el incremento de la piratería.

LEY 23 DE 1982: "Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente Ley y, en cuanto fuere compatible con ella, por el derecho común"[28].

Este trabajo de grado se respalda en la Ley 23 de 1982, la cual protege las opiniones expresadas y garantiza la protección de los derechos de autor.

---

[26] LEY 1273 DE 2009. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492. [citado mayo de 2014].

[27] LEY 603 DE 2000. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960. [citado junio de 2014].

[28] LEY 23 DE 1982. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431

2. METODOLOGÍA

2.1. PARADIGMA, ENFOQUE Y TIPO DE INVESTIGACIÓN

2.1.1. Paradigma de investigación. El trabajo de grado sigue un paradigma cuantitativo ya que usa datos, los recopila, los interpreta y los representa mediante datos y estadísticas, que permiten dar una visión mucho más objetiva del estado de la seguridad de la información en la empresa Expreso Juanambú.

Según Cauas (2006), "El Paradigma de Investigación Cuantitativa utiliza la recolección y el análisis de datos para contestar preguntas de investigación y probar hipótesis establecidas previamente y confía en la medición numérica, el conteo y frecuentemente en el uso de estadísticas para establecer con exactitud, patrones de comportamiento en una población. Se basa en un tipo de pensamiento deductivo, que va desde lo general a lo particular. Desde un conocimiento extenso de una generalidad, para luego deducir el comportamiento acotado de una particularidad individual. Se basa en un modelamiento que define cómo se hace cada cosa, transformándolo en un enfoque más rígido, enmarcado en una cierta forma de hacer las cosas"[29].

2.1.2. Enfoque de investigación. El enfoque de la investigación es de carácter cuantitativo, exploratorio y descriptivo. La recolección de información se llevará a cabo por medio de encuestas realizadas al personal que trabaja en la empresa Expreso Juanambú.

[29] CAUAS, Daniel, Elementos para la elaboración y ejecución de un proyecto de investigación, Guía para presentación de proyectos de investigación, Investigación en ciencias sociales, 2006, Disponible en: http://www.ninvus.cl/

2.1.3. Tipo de investigación. En la investigación que se realizó se utilizó el método exploratorio y descriptivo, primero se observó y se evaluó los aspectos claves de la empresa Expreso Juanambú y a través del enfoque cuantitativo y fundamentado en el método deductivo, se llevó a cabo la recolección y el análisis de los datos. El tipo de investigación exploratorio permitió obtener información y determinar aspectos investigativos hacia futuro. La investigación descriptiva permitió determinar las características fundamentales de la empresa Expreso Juanambú.

2.2. FUENTES DE RECOLECCIÓN DE INFORMACIÓN

Según Hernández, Fernández y Baptista (2006), citando a Dahnke, las fuentes primarias constituyen el objetivo de la investigación bibliográfica o revisión de la literatura y proporcionan datos de primera mano. Las fuentes secundarias son compilaciones, resúmenes y listados de referencias publicadas en un área de conocimiento en particular (son listados de fuentes primarias), es decir reprocesan información de primera mano[30].

2.2.1. Fuentes primarias. Como fuente de datos primarios se debe entender que son datos de primera mano, originales, producto de la investigación realizada sin intermediación de alguna naturaleza y se recolectaron específicamente con el fin de satisfacer las necesidades inmediatas de investigación. Los instrumentos que se utilizaron para recolectar la información fueron:

- Técnica de la observación.
- Entrevistas.

[30] HERNÁNDEZ, R., FERNÁNDEZ, C., BAPTISTA, P., Metodología de la Investigación 4ª Ed. McGraw Hill. 2006.

2.2.2. Fuentes secundarias. Los datos secundarios es toda aquella información que ha sido recopilada con anterioridad con un propósito diferente a la investigación, pero que permitió en gran medida ayudar a obtener información de la empresa Expreso Juanambú. Los datos e información se obtuvieron por medio de terceros. Entre las fuentes secundarias se obtuvo:

- Datos y documentos suministrados por los administradores de la empresa Expreso Juanambú.
- Textos académicos relacionados con la auditoría a la seguridad de la información.
- Artículos especializados de sistemas de control interno, control informático, auditoría de sistemas de información, protección y seguridad.

2.3. TÉCNICAS DE ANÁLISIS DE DATOS

En el siguiente trabajo de grado se llevaron a cabo diferentes técnicas e instrumentos para la recolección de los datos necesarios, estas fueron:

2.3.1. Observación directa. Hernández, Fernández y Baptista (2006), expresan que: "la observación directa consiste en el registro sistemático, válido y confiable de comportamientos o conducta manifiesta". A través de esta técnica el investigador puede observar y recoger datos mediante su propia observación[31].

A través de la observación directa se pudo identificar detalladamente el procedimiento que realiza el personal de Expreso Juanambú.

[31] HERNÁNDEZ, R., FERNÁNDEZ, C., BAPTISTA, P., Metodología de la Investigación 4ª Ed. McGraw Hill. 2006.

2.3.2. La entrevista. Se utilizó como instrumento de recolección de datos la entrevista, Corbetta (2007), opina que es una conversación provocada por un entrevistador con un número considerable de sujetos elegidos según un plan determinado con una finalidad de tipo cognoscitivo. Siempre está guiada por el entrevistador pero tendrá un esquema flexible no estándar[32].

Para este trabajo de grado la entrevista permitió conocer detalladamente los requerimientos de la empresa Expreso Juanambú, como funciona, con que elementos cuenta y a su vez identificar los riesgos, amenazas y vulnerabilidades más importantes en la empresa. (Ver ANEXO I - ENTREVISTAS).

2.3.3. Procesamiento de la información. El procesamiento de la información se realiza mediante la tabulación de datos, esta se realiza de forma mecánica empleando el uso de la computadora, estos datos se cargan directamente en un archivo creado en la aplicación Microsoft Office Excel 2010.

2.3.4. Análisis de la información. Luego de recopilados los datos que se obtienen como resultado de las diferentes técnicas aplicadas es necesario analizarlos de forma clara para así poder determinar cuáles son los requerimientos y necesidades. En el presente trabajo de grado se emplearon las siguientes técnicas de análisis:

2.3.4.1. Análisis cualitativo. Según Fernández y Baptista (2006), el análisis cualitativo se define como: "un método que busca obtener información de sujetos, comunidades, contextos, variables o situaciones en profundidad, asumiendo una postura reflexiva y evitando a toda costa no involucrar sus creencias o experiencia"[33].

[32] CORBETTA, P. *Metodología y técnicas de investigación.* Italia: McGraw-Hill. 2007.
[33] HERNÁNDEZ, R., FERNÁNDEZ, C., BAPTISTA, P., Metodología de la Investigación 4ª Ed. McGraw Hill. 2006.

En el presente trabajo de grado, el análisis cualitativo se aplica a las entrevistas realizadas donde el personal de la empresa Expreso Juanambú, expresa los requerimientos y deficiencias que cada área posee.

2.3.4.2. Análisis cuantitativo. Según, Sabino (2003), el análisis cuantitativo "se efectúa, naturalmente, con toda la información numérica resultante de la investigación. Esta, luego del procesamiento que ya se le habrá hecho, se nos presentará como un conjunto de cuadros, tablas y medidas, a las cuales se les han calculado sus porcentajes y presentado convenientemente"[34].

En el presente trabajo de grado el análisis cuantitativo será aplicado a las muestras seleccionadas, en este caso al inventario realizado en la empresa Expreso Juanambú. Con este análisis se determina cuáles son los activos más importantes y cuál será el plan de acción para el tratamiento de los riesgos.

2.4. PASOS METODOLÓGICOS EN EL PROCESO DE AUDITORÍA

La metodología para el proceso de auditoría a la empresa Expreso Juanambú consta de las siguientes fases:

FASE I: PLANEACIÓN

En la fase de planeación se realizaron las siguientes actividades:

1. Identificar el alcance y los objetivos de la auditoría a realizar.
2. Realizar el estudio inicial en la empresa Expreso Juanambú, para recolectar datos sobre el funcionamiento de la empresa.
3. Determinar los recursos necesarios para realizar la auditoría.

[34] SABINO, Carlos, El proceso de investigación, Ed. Panapo, Caracas, 1992

4. Elaboración del plan de trabajo.

FASE II: EJECUCIÓN

En la fase de ejecución se realizaron las siguientes actividades:

1. Elección dentro de los dominios del COBIT de los procesos a auditar.
2. Ejecutar la auditoría.
3. Elaboración de un análisis de hallazgos y riesgos que permitan identificar cuáles de las actividades identificadas tienen una menor eficiencia, cuáles de los procesos tienen mayor impacto dentro del sistema (ejecución de la auditoría).
4. Elaboración de un informe con los hallazgos y los riesgos encontrados, detectando las causas y su efecto.
5. Elaboración del modelo de madurez en el cual se encuentra el sistema auditado.

FASE III: CONSOLIDACIÓN DEL INFORME FINAL

En esta etapa del proceso de auditoría se presenta un informe detallado y especifico al gerente de Expreso Juanambú y al jefe de sistemas sustentando donde se dan a conocer los problemas encontrados y se sugieren posibles soluciones.

3. RESULTADOS DEL PROCESO DE AUDITORÍA

3.1. IDENTIFICACIÓN DEL ENTORNO AUDITABLE

3.1.1. Área gerencia. La gerencia es la encargada de verificar que todos los procedimientos se cumplan correctamente, también es la delegada de ejecutar y hacer cumplir las decisiones emanadas por la Junta Directiva, también dirige y coordina reuniones, asiste a programas o conferencias que conlleven al fortalecimiento y mejoramiento de la calidad de la prestación de servicios.

Los recursos auditables en esta área fueron: el personal y recursos físicos de oficina.

No se evaluaron recursos tecnológicos ya que no se disponen de ellos, es decir, no se manejan aplicaciones de ninguna clase ni existen computadores asignados a ésta área.

3.1.2. Área secretaría. La secretaría es la encargada de la atención al cliente, recepción de documentos, cancelación de contratos, otras funciones para vehículos y propietarios del parque automotor.

Los recursos auditables en esta área fueron: el personal, equipos de cómputo, sistemas operativos, laptops y oficinas.

3.1.3. Área revisoría fiscal. La revisoría fiscal es la encargada de revisar que la contabilidad se encuentre al día y generar un dictamen sobre los estados financieros.

Los recursos auditables en esta área fueron: el personal, equipos de cómputo, sistemas operativos, laptops y oficinas.

3.1.4. Área telemática. El área de telemática es la encargada de la administración y el mantenimiento de recursos informáticos.

Los recursos auditables en esta área fueron: el personal, equipos de cómputo, sistemas operativos, laptops, oficinas, servidores, bases de datos, redes, switch, router y cámaras de seguridad.

3.1.5. Área radiocomunicaciones. El área de radiocomunicaciones es la encargada de administrar la central de comunicaciones en su respectivo turno, atender diligentemente las solicitudes de servicio de los usuarios o clientes de radio teléfono.

Los recursos auditables en esta área fueron: el personal, equipos de cómputo, sistemas operativos, laptops y oficinas.

3.1.6. Área caja y tesorería. El área de caja y tesorería es la encargada de registrar el recaudo de ingresos diariamente que se genera en la empresa.

Los recursos auditables en esta área fueron: el personal, equipos de cómputo, sistemas operativos, laptops y oficinas.

3.1.7. Área lubricentro y monta llantas. El área de lubricentro y monta llantas es la encargada del mantenimiento de los vehículos, es responsable del inventario y maquinaria que hacen parte del centro de lubricación.

Los recursos auditables en esta área fueron: el personal encargado del mantenimiento de los vehículos del parque automotor y oficinas.

3.2. ANÁLISIS Y EVALUACIÓN DE RIESGOS

Para la elaboración de este proyecto se utilizó la metodología MAGERIT, esta metodología permite determinar el impacto sobre un activo de información, con la pérdida de confidencialidad, integridad y disponibilidad derivado de la materialización de las amenazas junto con las vulnerabilidades que pueden ser explotadas por esas amenazas, se determina la probabilidad de ocurrencia de dichas amenazas, se calcula el riesgo actual frente a las amenazas, y se determina el riesgo residual, resultante luego de que se implementen los controles.

3.2.1. Análisis del entorno auditable. Para el análisis y evaluación de riesgos se realizaron visitas a las instalaciones de la empresa Expreso Juanambú, y específicamente a las instalaciones de las aulas de cómputo, además de la aplicación de instrumentos como listas de chequeo o checklist de verificación y cuestionarios al personal de la administración de los recursos tecnológicos también se realizaron entrevistas a los empleados.

Aparte de de estos instrumentos se utilizó la observación directa como método para determinar y percibir los aspectos relacionados con el desarrollo de actividades y así poder llegar a evaluar el cumplimiento, fallas, vulnerabilidades y riesgos a los que estaba sometido las operaciones llevadas a cabo en la empresa.

La observación se inicia con el acceso a las instalaciones para definir cuál es el procedimiento de entrada y salida del personal y de las personas.

FIGURA 7. ESCALERA DE ACCESO A LAS INSTALACIONES

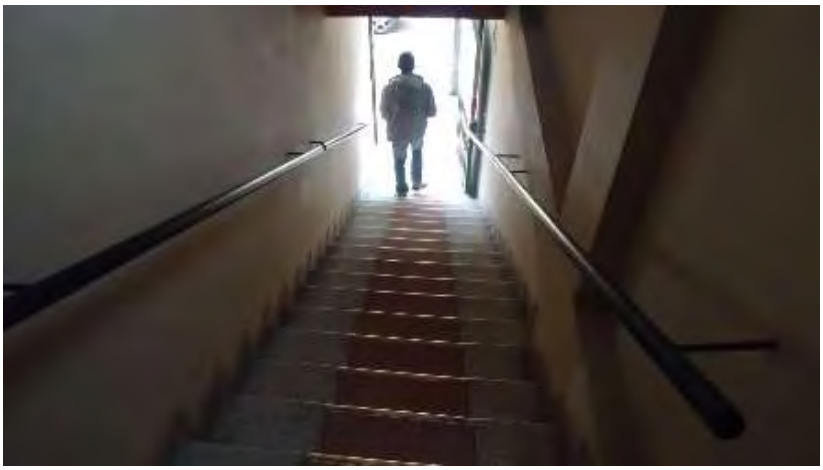
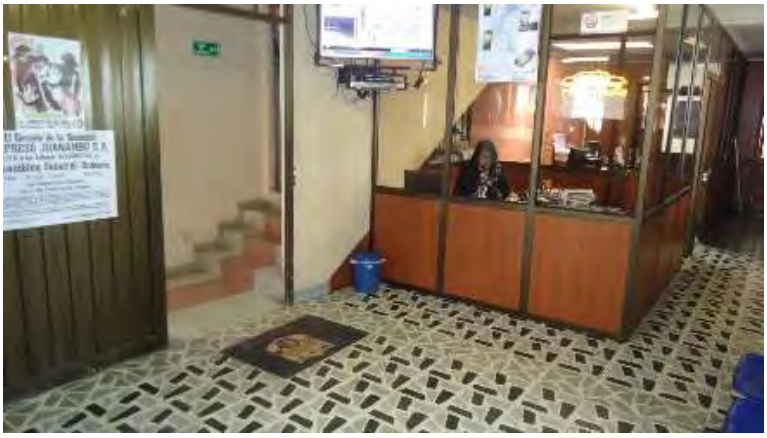


FIGURA 8. ACCESO A LA TERRAZA DE LAS INSTALACIONES

FIGURA 9. ACCESO PRINCIPAL A LAS INSTALACIONES

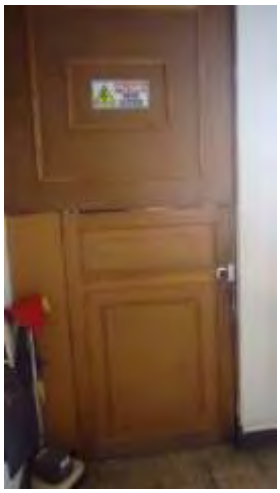


En las figuras 7, 8 y 9, se evidencia que no existe un control de ingreso por parte de un guarda de seguridad o algún empleado de la organización encargado de la vigilancia a la entrada principal de las instalaciones.

Además, no se implementa un sistema de monitoreo de ruido, algún dispositivo de alerta o alarma para accesos a las instalaciones en horas de no operatividad.

Después se procede a verificar donde están localizados los servidores y como es el procedimiento de acceso a ellos.

FIGURA 10. CUARTO DE SERVIDORES



En la Figura 10, queda evidenciado que el acceso a la sala de servidores no se encuentra con las medidas apropiadas de seguridad, su acceso no es restringido, cualquier persona puede entrar fácilmente a la sala de servidores y manipularlos de forma incorrecta o incluso robarlos.

Posteriormente, se comprueba si la empresa cuanta con cámaras de seguridad y cuál es el procedimiento para el monitoreo de las mismas.

FIGURA 11. CÁMARAS DE SEGURIDAD

FIGURA 12. MONITOREO CÁMARAS DE SEGURIDAD

Uno de los puntos a favor en los temas de seguridad que tiene la organización es contar con un sistema de monitoreo por cámaras de seguridad. Se monitorea la entrada principal, las instalaciones del Lubricentro, la entrada principal que da a la vía pública y la entrada del público a las instalaciones de la organización, evidenciado en las figuras 11 y 12. Se tiene un registro detallado de todas las actividades realizadas en la empresa.

A continuación, se comprueba si la empresa cuenta con una fuente de poder ininterrumpida, como es el funcionamiento de ella y donde está localizada.

FIGURA 13. SISTEMA DE FUENTE DE PODER ININTERRUMPIDA

En la Figura 13, se encontró un sistema de fuente de poder Ininterrumpida casera. De buen funcionamiento, pero no se establece su posición en un lugar seguro contra inundaciones ya que este recinto se ubica en la terraza de las instalaciones de la Empresa.

Después, se observa cómo está organizado el cableado estructurado en la empresa Expreso Juanambú.

FIGURA 14. CABLEADO ESTRUCTURADO

FIGURA 15. CABLEADO ESTRUCTURADO 2

FIGURA 16. CABLEADO ESTRUCTURADO 3

En las Figuras 14, 15 y 16, se ponen en evidencia que el cableado estructurado no está ubicado de forma adecuada, se ha instalado sin seguir el lineamiento de los estándares de seguridad para la manipulación de cableado estructurado.

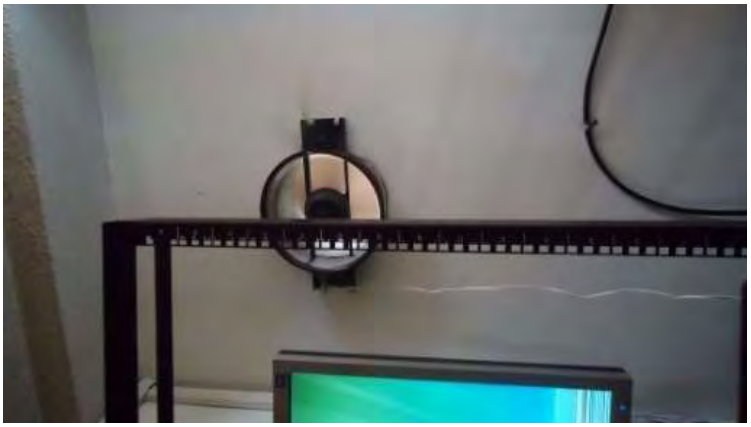
Posteriormente, se revisa si en la empresa existe documentación física y como está organizada.

FIGURA 17. DOCUMENTACIÓN SECRETARÍA

A pesar del buen manejo y el orden que se tiene en la administración de archivos de forma manual, los documentos se encuentran expuestos a riesgos de incendio o inundación y por lo tanto a un gran volumen de pérdida de información, ya que no existen extintores ni alarmas contra incendio.

A continuación, se verifica si existe un sistema de ventilación en las oficinas, especialmente en el servidor y como es el funcionamiento.

FIGURA 18. IMPLEMENTACIÓN SISTEMA DE VENTILACIÓN



En la figura 18, se observó que la organización Implementó un sistema de ventilación por recomendación del equipo de esta auditoría para salvaguardar los equipos que se encuentran en el cuarto de servidores de la empresa frente a las altas temperaturas que estos equipos emiten.

Después se revisa el funcionamiento del servidor, que sistema operativo tiene, cual es el manejo del servidor, quien lo manipula.

FIGURA 19. SERVIDOR PRINCIPAL

FIGURA 20. SERVIDOR PRINCIPAL 2

En las Figuras 19 y 20, se encontró que el servidor principal de la empresa en el cual se venía trabajando tenía un sistema operativo Windows XP, con equipamiento obsoleto y por recomendación de los estudiantes auditores la empresa invirtió en nuevos equipos con Sistemas Linux que son más estables y seguros.

El análisis de riesgos es una aproximación sistemática para determinar el riesgo siguiendo unos pasos:

3.2.2. Definición y valoración de activos de información. Por medio de un inventario conformado por los activos de información a proteger y cuyas dimensiones de valoración para cada uno de estos son: confidencialidad, integridad y disponibilidad.

Los activos de información se clasificaron así:

TABLA 1. ACTIVOS DE INFORMACIÓN

[D] Datos / Información
[S] Servicios
[SW] Software / Aplicativos
[HW] Hardware / Equipos informáticos
[COM] Redes de comunicaciones
[Media] Soportes de información
[AUX] Equipamiento auxiliar
[L] Instalaciones
[P] Personal
[SI] Sistema de Información

Fuente: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – MAGERIT Versión 3.0

Para ver la lista completa de activos de información dirigirse al ANEXO F - INVENTARIO DE ACTIVOS DE INFORMACIÓN.

3.2.3. Identificación de amenazas a que están expuestas los activos de información. Aquí se identificaron y evaluaron las amenazas que sufren los activos de información de la empresa Expreso Juanambú.

Clasificación de amenazas según MAGERIT:

TABLA 2. AMENAZAS SEGÚN MAGERIT

[N]	**Desastres naturales**
N01	Fuego
N02	Daños por agua
[I]	**De origen industrial**
I01	Fuego
I02	Daños por agua
I03	Contaminación mecánica
I04	Contaminación electromagnética
I05	Avería de origen físico o lógico
I06	Corte del suministro eléctrico
I07	Condiciones inadecuadas de temperatura y/o humedad
I08	Fallo de servicios de comunicaciones
I09	Interrupción de otros servicios y suministros esenciales
I10	Degradación de los soportes de almacenamiento de la información
I11	Emanaciones electromagnéticas
[E]	**Errores y fallos no intencionados**
E01	Errores de los usuarios
E02	Errores del administrador
E03	Errores de monitorización (logs)
E04	Errores de configuración
E07	Deficiencias en la organización
E08	Difusión de software dañino
E09	Errores de [re]encaminamiento
E10	Errores de secuencia

E14	Escapes de información
E15	Alteración de la información
E16	Introducción de información incorrecta
E17	Degradación de la información
E18	Destrucción de información
E19	Divulgación de información
E19	Divulgación de información
E20	Vulnerabilidades de los programas
E21	Errores de mantenimiento / actualización de programas
E23	Errores de mantenimiento / actualización de equipos (hardware)
E24	Caída del sistema por agotamiento de recursos
E28	Indisponibilidad del personal
[A]	**Ataques intencionados**
A04	Manipulación de la configuración
A05	Suplantación de identidad de usuario
A06	Abuso de privilegios de acceso
A07	Uso no previsto
A08	Difusión de software dañino
A09	Encaminamiento de mensajes
A10	Alteración de secuencia (de mensajes)
A11	Acceso no autorizado (aprovechando una debilidad)
A12	Análisis de tráfico
A13	Repudio
A14	Interceptación de información (escucha)
A15	Modificación de la información
A16	Introducción de falsa información

A17	Corrupción de la información
A18	Destrucción la información
A19	Divulgación de información
A22	Manipulación de programas
A24	Denegación de servicio
A25	Robo
A26	Ataque destructivo
A27	Ocupación enemiga
A28	Indisponibilidad del personal
A29	Extorsión
A30	Ingeniería social

Fuente: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – MAGERIT Versión 3.0

Para ver la lista de amenazas presentes en la empresa Expreso Juanambú dirigirse al ANEXO G - ANÁLISIS Y EVALUACIÓN DE RIESGOS.

3.2.4. Identificación de vulnerabilidades existentes para los activos de información. Se identificaron las vulnerabilidades que pueden ser explotadas por las amenazas potenciales por medio de inspección visual, listas de verificación, revisión de la información suministrada.

La clasificación de vulnerabilidades existentes en los activos de información fue la siguiente:

TABLA 3. VULNERABILIDADES EN LOS ACTIVOS DE INFORMACIÓN

PROCESO	CUSTODIO	
	Principal	**Alterno**
Tesorería	Gerente	Jefe de telemática
Secretaria	Gerente	Jefe de telemática
Revisoría fiscal	Gerente	Jefe de telemática
Telecomunicaciones	Gerente	Jefe de telemática

Para ver la lista completa de vulnerabilidades de activos de información ver ANEXO F - INVENTARIO DE ACTIVOS DE INFORMACIÓN.

3.2.5. Estimación del impacto. El objetivo es conocer el alcance del daño producido en la empresa Expreso Juanambú derivado de la materialización de las amenazas sobre los activos de información.

La estimación del impacto se desarrolló con base a MAGERIT.

TABLA 4. ESTIMACIÓN DE IMPACTO

IMPACTO		***Degradación***		
		1%	50%	100%
Valor del activo	Muy Alto	3	5	8
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2

	Muy Bajo	1	1	1

Fuente: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – MAGERIT Versión 3.0

Para ver la clasificación del impacto producido ver el ANEXO G - ANÁLISIS Y EVALUACIÓN DE RIESGOS para cada uno de los activos de información.

3.2.6. Estimación de la probabilidad. El objetivo consiste en estimar la frecuencia de materialización de una amenaza en función de la cantidad de veces que esta pueda ocurrir.

La estimación de la probabilidad se desarrolló con base a MAGERIT.

TABLA 5. ESTIMACIÓN DE PROBABILIDAD

1	Raro	Puede ocurrir una vez cada 2 años.
2	Muy baja	Al año.
3	Baja	En 6 meses.
4	Media	Al mes.
5	Alta	A la semana.

Fuente: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – MAGERIT Versión 3.0

Para ver la estimación de la probabilidad ver el ANEXO G - ANÁLISIS Y EVALUACIÓN DE RIESGOS para cada uno de los activos de información.

3.2.7. Estimación del riesgo. La estimación del riesgo es obtenida por medio de la siguiente ecuación matemática:

Riesgo = probabilidad x impacto

3.3. GESTIÓN DE RIESGOS

3.3.1. Plan de tratamiento de riesgos. Contiene una serie de controles y recomendaciones básicas de seguridad para toda la organización que permita disminuir un alto grado de riesgo.

3.3.2. Establecer normativa para controlar el riesgo. La información es un activo que tiene valor para la empresa y por consiguiente debe ser protegida y resguardada adecuadamente, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo así, a una mejor gestión de la empresa.

Por lo tanto, resulta necesario la elaboración de una Política de Seguridad de la Información que hagan parte de la cultura organizacional de la empresa Expreso Juanambú, lo que implica que debe contarse con el manifiesto compromiso de todos los funcionarios de una manera u otra vinculados a la gestión, para contribuir a la difusión, consolidación y cumplimiento.

3.4. EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN CUANTO A HARDWARE, SOFTWARE E INSTALACIONES

3.4.1. Hardware. El hardware evaluado en la empresa Expreso Juanambú fueron los equipos más utilizados y los más importantes de la empresa, para ello se realizó una lista de activos, después se clasifico estos activos para determinar el grado de importancia y por último se comprobó de manera particular cuales son las amenazas más significativas que puede sufrir este activos para realizar una evaluación del riesgo.

En general, el hardware administrado en la empresa Expreso Juanambú cuenta con una buena gestión, se realiza un mantenimiento periódico y se manipula adecuadamente.

Recomendaciones: se debe realizar la verificación de hardware y software para garantizar la compatibilidad con los otros componentes del sistema de la empresa. Además, se debe contar con la documentación antes de la evaluación de los requerimientos del negocio.

3.4.2. Software. La empresa Expreso Juanambú no es una empresa dedicada al desarrollo de software, por este motivo se determinó cuáles son los programas más utilizados en la empresa, como es el procedimiento para la adquisición de software especializado y cuáles son las licencias de los programas que ellos usan.

En general, el software administrado en la empresa Expreso Juanambú cuenta con una buena gestión, se realiza un mantenimiento periódico y se manipula adecuadamente.

Recomendaciones: el encargado de administrar recursos TI debe realizar un mantenimiento preventivo a recursos TI, para asegurar que estos funcionen correctamente y no presenten fallos a la hora del uso además, debe asegurar la información instalando software especializado para prevenir spyware y malware en los computadores.

El jefe de sistemas debe crear políticas de instalación de software y operación de equipos, para que las personas no instalen software innecesario y operen bien los equipos, debe instalar software especializado para detectar accesos no autorizados al sistema.

3.4.3. Instalaciones. Se realizó una evaluación a toda la empresa y se encontró algunos fallos de seguridad en las instalaciones debido al poco compromiso adquirido en la empresa y la confianza que se genera al no reportar incidentes de seguridad.

Las instalaciones de Expreso Juanambú no son las más adecuadas, pero cumplen con el objetivo de brindar la atención a los clientes.

Recomendaciones: todos los empleados de la empresa y, cuando se considere oportuno, los usuarios externos y los terceros que desempeñen funciones dentro de la empresa, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos. Esto comprende los requisitos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información, el uso correcto de los recursos en general; como por ejemplo su estación de trabajo y del mantenimiento de los equipos de cómputo utilizados.

El gerente debe afiliarse a una compañía de seguridad para salvaguardar la integridad de la empresa y sus empleados, debe crear políticas de ingreso a oficinas y a instalaciones.

El gerente debe crear políticas de ingreso a las instalaciones manejando unas bitácoras de acceso, asegurar los equipos, realizar un mantenimiento a la infraestructura y certificarse con normas de calidad.

3.5. INFORME FINAL DE AUDITORÍA

De acuerdo a los hallazgos y evidencias encontradas en la empresa Expreso Juanambú se realizó un informe final de auditoría en el cual se pueden destacar los aspectos más importantes de seguridad que maneja la empresa y una serie de

recomendaciones que se debe realizar para que la empresa logre mejorar en aspectos específicos de seguridad. (Ver ANEXO L - INFORME FINAL DE AUDITORÍA).

4. CONCLUSIONES

En una empresa la información, los procesos, sistemas y redes son activos muy importantes. Definir, lograr, mantener y mejorar la seguridad de la información es esencial para la operación de las actividades empresariales.

Actualmente las empresas, sus sistemas e información enfrentan amenazas de seguridad por eso es importante implementar políticas de seguridad de la información para evitar y reducir los riesgos relevantes.

La implementación de COBIT e ISO/IEC 27000 en una empresa ayudará a mejorar la calidad, fiabilidad y los servicios de TI también se reducirá los riesgos, incidentes, y fallas en los procesos.

Para poder alinear COBIT e ISO/IEC 27000 en primer lugar se deben ajustar a los requisitos del negocio y ser integradas entre sí con los procedimientos internos. COBIT ofrece un marco de control e ISO/IEC 27000 incluye áreas específicas y pueden ser mapeadas en el marco COBIT.

Con la metodología MAGERIT se puede realizar un análisis de los riesgos que implica la evaluación del impacto que puede afectar a la seguridad de la información en una organización; Identificando riesgos y amenazas que pueden vulnerar el sistema. La obtención de los resultados de este análisis permite generar recomendaciones que se deben adoptar para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir su impacto.

5. RECOMENDACIONES

Indagar sobre otros aspectos relacionados con la investigación.

Incentivar a las empresas auditadas a implantar las recomendaciones pertinentes.

Elaborar programas de capacitación para los empleados de la empresa Expreso Juanambú.

Administrar de forma correcta toda la información presente en la empresa Expreso Juanambú.

Conocer muy bien el funcionamiento de la empresa y recolectar la mayor cantidad de información.

Tener en cuenta las diferencias de los enfoques y detalles que manejan COBIT e ISO/IEC 27000.

Usar MAGERIT ya que es una metodología muy amplia con la posibilidad de minimizar los riesgos y está relacionada con las tecnologías de la información.

6. INFORME EJECUTIVO

Señor:
Bolívar Benavides Lagos.
Gerente general empresa Expreso Juanambú.

Una vez finalizada la auditoria a la empresa Expreso Juanambú y partiendo del objetivo de evaluar la seguridad de la información en cuanto a hardware, software e instalaciones, con procesos de auditoría basada en los estándares COBIT e ISO/IEC 27000, con el propósito de establecer recomendaciones, que permitan la definición de políticas, procesos y procedimientos de la organización Expreso Juanambú con el proposito de auditar la seguridad de la información en las áreas de secretaria, revisoría fiscal, telecomunicaciones, telemática, tesorería, lubricentro, evaluando el hardware, software e instalaciones en cada una de estas áreas.

Se encontraron los siguientes hallazgos positivos:

- El personal que trabaja en la empresa Expreso Juanambú se encuentra capacitado para cumplir sus funciones responsablemente.
- La estructura jerárquica de la empresa posee un sistema administrativo bien organizado, en el cual se tiene identificados sus usuarios y las necesidades de servicio.
- La dirección de la empresa cuanta con un grado de responsabilidad alto para la toma de decisiones, se encuentra una actitud favorable de parte de las autoridades superiores para desarrollar sus actividades de manera pertinente.
- Se percibe un ambiento de trabajo éticamente propicio con relación a la administración del personal. El clima laboral es de una colaboración altamente profesional entre todos sus empleados.

- La dirección se encuentra abierta a posibilidades de expansión y mejoramiento empresarial.

Como consecuencia de la auditoría realizada se sugiere aplicar las siguientes recomendaciones:

- Todos los empleados de la empresa y cuando se considere oportuno, los usuarios externos y los terceros que desempeñen funciones dentro de la empresa, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos. Esto comprende los requisitos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información, el uso correcto de los recursos en general; como por ejemplo su estación de trabajo y del mantenimiento de los equipos de cómputo utilizados.
- Se debe realizar la verificación de hardware y software para garantizar la compatibilidad con los otros componentes del sistema de la empresa.
- Restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.
- El gerente debe ordenar la creación de un plan de contingencia para los recursos TI, el cual debe ser creado por el jefe de sistemas.
- El gerente debe afiliarse a una compañía de seguridad para salvaguardar la integridad de la empresa y sus empleados, debe crear políticas de ingreso a oficinas y a instalaciones.
- El encargado de administrar recursos TI debe realizar un mantenimiento preventivo a recursos TI, para asegurar que estos funcionen correctamente y no presenten fallos a la hora del uso además, debe asegurar la información instalando software especializado para prevenir spyware y malware en los computadores.

- El jefe de sistemas debe aislar el cableado estructurado para que cuente con alguna protección y que cumpla con estándares de calidad y seguridad, debe crear políticas para la administración de computadores, debe administrar los puertos de acceso, para que el sistema no se vulnere fácilmente, debe limitar la conexión al sistema para que no todas las personas puedan entrar a él.
- El jefe de sistemas debe crear políticas de instalación de software y operación de equipos, para que las personas no instalen software innecesario y operen bien los equipos, debe instalar software especializado para detectar accesos no autorizados al sistema.

En consideración a la auditoría realizada por los estudiantes Alvaro Ronald Eraso Ceron e Ivan David Guerrero Arellano, concluimos que la empresa Expreso Juanambú de acuerdo al análisis y evaluación de riegos de activos de información tiene un riesgo actual en una escala tolerable y una estimación del impacto moderada, esto quiere decir que la seguridad de la información tiene un nivel de confidencialidad de uso interno, un nivel de integridad normal y un nivel de disponibilidad media.

BIBLIOGRAFÍA

ACEITUNO CANAL, Vicente “Seguridad de la Información: expectativas, riesgos y técnicas de protección”, Ed Noriega Editores. México. D.F. 2006.

ARTERO, J.L, Seguridad en la Información, Ediciones Paraninfo S.A, Madrid, 2008.

CANO, J; JEIMY, J, Inseguridad de la Información, S.A. Marcombo, Barcelona, 2013.

CAUAS, Daniel, Elementos para la elaboración y ejecución de un proyecto de investigación, Guía para presentación de proyectos de investigación, Investigación en ciencias sociales, 2006, Disponible en: http://www.ninvus.cl/

CEPEDA ALONSO, Gustavo, Auditoría y Control Interno, Mc GRAW – HILL, México D.F., 1997.

CORBETTA, P. Metodología y técnicas de investigación, Italia: McGraw-Hill, 2007.

CORLETTI ESTRADA, Alejandro, Seguridad Por Niveles, DarFe Learning Consulting S.L, Madrid, 2011.

DALTABUIT GODÁS, Enrique, VÁZQUEZ, José de Jesús, La Seguridad de la Información. Limusa Noriega Editores, México, 2007. pág. 215.

ECHENIQUE, José Antonio, Auditoría en Informática. Ed. Mc GRAW – HILL, 2001.

GÓMEZ VIEITES, Álvaro, Enciclopedia de la seguridad informática, Alfa Omega grupo editor, México, Primera edición, 2007, pág. 4; pág. 18.

HERNÁNDEZ, R., FERNÁNDEZ, C., BAPTISTA, P., Metodología de la Investigación 4ª Ed. McGraw Hill. 2006.

KIM & SOLOMON, David, Michael G, Fundamentals of information systems security, Jones and Bartlett learning, 1st edition, 2010.

LAZCANO SERES, Juan M, El Manejo de las Organizaciones, su Auditoría y su Control, Mc GRAW-HILL, México D.F., 1997.

NEWMAN, Robert C, Computer Security protecting digital resources. Jones and Bartlett Publisher, 2010.

PAREDES FIERRO, Geomayra Alexandra, VEGA NOBOA, Mayra Alexandra, Desarrollo de una Metodología para la Auditoría de Riesgos Informáticos (físicos y lógicos) y su aplicación al Departamento de Informática de la Dirección Provincial de Pichincha del Consejo de la Judicatura", Tesis Escuela Superior Politécnica de Chimborazo Facultad de Informática y Electrónica, Riobamba, 2011, p. 109

PIATTINI, Mario, DEL PESO Emilio, Auditoría en Informática: Un enfoque práctico, Alfaomega / RA-MA, México D.F., 2001.

PIATTINI, Mario, Auditoría de Tecnologías y Sistemas de Información, RA-MA, México D.F, 2008.

SABINO, Carlos, El proceso de investigación, Ed. Panapo, Caracas, 1992.

NETGRAFIA

ALINEANDO COBIT®4.1, ITIL®V3 E ISO/IEC 27002 EN BENEFICIO DE LA EMPRESA. [en línea]. [citado enero de 2014]]. Disponible en: http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf

EL PORTAL DE ISO 27001 EN ESPAÑOL. [en línea]. Actualizada 21 de noviembre de 2013. [citado enero de 2014]. Disponible en: http://www.iso27000.es/

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION, Inc. [US] [en línea]. Actualizada: 21 de noviembre de 2013. [citado enero de 2014]. Disponible en: https://www.isaca.org/Pages/default.aspx

ISO/IEC 27000:2012. [en línea]. Actualizada 21 de noviembre de 2013. [citado enero de 2014]. Disponible en: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56891

DECRETO 1377 DE 2013. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646. [Citado enero de 2014].

DECRETO 2693 DE 2012. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51198. [Citado enero de 2014].

EL PORTAL DE ISO 27001 EN ESPAÑOL. [en línea] Disponible en internet. http://www.iso27000.es/iso27000.html. [Citado enero de 2014].

ISO 27002. [en línea] Disponible en internet. http://iso27002.es/. [Citado marzo de 2014].

LEY 1341 DE 2009. [en línea] Disponible en internet. http://www.mintic.gov.co/portal/604/w3-article-3707.html. [Citado marzo de 2014].

LEY ESTATUTARIA 1581 DE 2012. [en línea] Disponible en internet. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. [Citado marzo de 2014].

LEY 1273 DE 2009. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492.[Citado marzo de 2014].

LEY ESTATUTARIA 1266 DE 2008. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488.[Citado marzo de 2014].

LEY 603 DE 2000. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960.[Citado marzo de 2014].

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. [en línea] Disponible en internet. https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_I_ metodo.pdf. [Citado julio de 2014].

SEGURIDAD INFORMÁTICA. [en línea] Disponible en internet. http://seguridadinformaticaufps.wikispaces.com/. [Citado julio de 2014].

SEGURIDAD DE LA INFORMACIÓN EN COLOMBIA. [en línea] Disponible en internet. http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html. [Citado julio de 2014].

ITIL®-Gestión de Servicios TI. [en línea] Disponible en internet. http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/vision_general_gestion_servicios_TI/vision_general_gestion_servicios_TI.php [Citado julio de 2014].

ISO 27002. [en línea] Disponible en internet. https://iso27002.wiki.zoho.com/. [Citado julio 2014].

SITIO WEB DE SEGURIDAD PARA TI BASADO EN COBIT. [en línea] Disponible en internet. http://redyseguridad.fip.unam.mx/proyectos/cobit/seccion_informativa/4_monitorear_evaluar/monitorear_evaluar_02/2_me02_obj_con.html. [Citado julio 2014].

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SGSI. [en línea] Disponible en internet. http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/capitulo_3__analisis_de_riesgos.html [citado julio 2014].