UNIVERSIDAD NACIONAL AUTONOMA DE NICARAGUA, MANAGUA

UNAN-MANAGUA

FACULTAD DE CIENCIAS ECONOMICAS

DEPARTAMENTO DE CONTADURIA PÚBLICA Y FINANZAS

SEMINARIO DE GRADUACIÓN PARA OPTAR AL TÍTULO DE LICENCIADO EN CONTADURÍA PÚBLICA Y FINANZAS

TEMA:

NORMAS INTERNACIONALES DE AUDITORÍA (NIA)

SUB TEMA:

ANALISIS DEL SISTEMA DE CONTROL INTERNO DE TECNOLOGÍAS DE LA INFORMACIÓN (TI) APLICANDO EL MARCO NORMATIVO COBIT 5.0 EN LA ENTIDAD NP ENTERPRISE INC. AL 31 DE DICIEMBRE 2016, SEGÚN LA NORMA INTERNACIONAL DE TRABAJOS DE ASEGURAMIENTO SOBRE LOS CONTROLES DE UNA ORGANIZACIÓN DE SERVICIO NITA 3402

TUTOR:

MSC. DAVID FRANCISCO ALVARADO DÁVILA

AUTORES:

BR. HÉCTOR ALEJANDRO SALGADO PALACIOS

BR. MICHAEL BILLY TEJEDA VALENZUELA

MANAGUA, FEBRERO 2018

i. Dedicatoria

El presente trabajo lo dedico primeramente a Dios por haberme dado fortaleza y sabiduría en el transcurso de mis estudios, a mis padres: Alba Azucena Palacios Zelaya y Jairo Ramón Palacios Serrano, por su esfuerzo y sacrificio a quienes debo mi formación profesional, a mis maestros por haberme transmitido todos los conocimientos necesarios que han sido de mucha ayuda durante estos cinco años de carrera, a mis compañeros de clases quienes me han brindado su amistad incondicional, mis maestros en todo lo largo de mi formación profesional, en especial al MSC. David Francisco Alvarado Dávila, por brindarnos su ayuda y apoyo incondicional y transmitirnos todos los conocimientos necesarios para mi desarrollo profesional.

Br. Héctor Alejandro Salgado Palacios.

i. Dedicatoria

Primeramente, a Dios por haberme dado fuerza, valor, sabiduría y comprensión en cada una de las etapas de mi formación profesional, logrando llegar hasta este momento de mi carrera y elaboración de este seminario, y también por su infinita bondad y amor.

A mi madre, Rosa Azucena por cada consejo, ayuda, cada palabra de aliento y motivación, por los valores inculcados y cada muestra de su amor incondicional, para lograr cada sueño y meta que me proponía siendo esta una de tantas en las que voy a tener a mi lado al ser que ha dado su vida por mi

A mi padre, Guillermo Justino por ser un padre ejemplar, una persona llena de sabiduría que cada día con frases y consejos las transmitía a mí para formar a un profesional de calidad, su apoyo incondicional y amor que demostraba cada día con sus palabras.

A mis hermanos Douglas y William que siempre han estado presente apoyándome y aportando cada día para lograr todos los objetivos, participando directa e indirectamente cada día. A mis tías Georgina y Mari Luz y demás familiares ya que sin sus enseñanzas nada de esto hubiese sido posible

Y a mis compañeros y profesores, con mención especial al MSC. David Francisco Alvarado Dávila, por transmitirme todos los conocimientos posibles y guiarme en mi desarrollo profesional como contador.

Br. Michael Billy Tejeda Valenzuela

ii. Agradecimiento

A Dios por darme la fuerza, perseverancia para llegar hasta el final del cierre de mi seminario de graduación; a mis padres Alba Azucena Palacios Zelaya y Jairo Ramón Palacios Serrano por enseñarme a cultivar los valores de la vida, uno de ellos es el respeto a mis semejantes, a las personas que me quieren y me brindan su amistad incondicional y me dan un lugar en sus vidas, a mi tutor M.sc. David Francisco Alvarado Dávila por brindarnos sus conocimientos, ayuda, paciencia, comprensión y apoyo incondicional para realizar el seminario de graduación.

Br. Héctor Alejandro Salgado Palacios.

ii. Agradecimiento

Primeramente, a Dios, por haberme permitido llegar hasta este momento de mi vida académica y profesional, a mis padres, Rosa Azucena y Guillermo Justino, por instarme a ser una persona de bien, de buenos valores y demostrarme cada día lo que en verdad uno puede valer en la vida.

A mis hermanos, familiares y amistades en especial a mis compañeros: Hector Alejandro Salgado Palacios, Melvin Oporta Villalta y Esther Gabuardi Hernández, ya que ellos me han brindado en todo este tiempo una muestra de su amistad incondicional en todos los momentos fáciles y difíciles que hemos pasado a lo largo de la carrera,

A todos y cada uno de los maestros que he tenido en mi vida académica, ya que ellos aportaron un pequeño grano de sabiduría y conocimiento, en especial a mis maestros de pregrado de la UNAN-RUCFA, por forjar a un futuro profesional de calidad.

Br. Michael Billy Tejeda Valenzuela

iii. Valoración del docente

MSC. Álvaro José Guido Quiroz Viernes, 16 de febrero del 2018

Director de Departamento de Contaduría Pública y Finanzas

Facultad de Ciencias Económicas

Su Despacho.

Estimado Maestro:

Remito a usted los ejemplares del Informe Final de Seminario de Graduación titulado con el tema general: Normas Internacionales de Auditoría y el sub-tema "Análisis del sistema de control interno de tecnologías de la información (TI) aplicando el marco normativo COBIT 5.0 en la entidad NP Enterprise Inc. Al 31 de diciembre 2016, según la Norma internacional de trabajos de aseguramiento sobre los controles de una organización de servicio NITA 3402". presentado por los bachilleres: Héctor Alejandro Salgado Palacios, Carnet No. 13-20696-5 y Michael Billy Tejeda Valenzuela, Carnet No 13-20802-1, para optar al título de Licenciado en Contaduría Pública y Finanzas.

Este Informe Final reúne todos los requisitos metodológicos para el Informe de Seminario de Graduación que especifica la Normativa para las modalidades de Graduación como formas de culminación de estudios, Plan 2013, de la Unan-Managua, solicito a usted fijar fecha de defensa según lo establecido para tales efectos.

Sin más que agregar al respecto, deseándole éxitos en sus funciones, aprovecho la ocasión para reiterar mis muestras de consideración y aprecio.

_____

MSC. David Francisco Alvarado Dávila

Docente Tutor

iv. Resumen

En tiempos de constantes avances tecnológicos muchas organizaciones invierten recursos en tecnología para desarrollar sus objetivos y capacidades de entorno empresarial, todas ellas están expuestas a riesgos e impactos potenciales debido a vulnerabilidades en sus controles, procesos y proyectos empresariales; por ello la importancia de analizar los controles y procesos de la información financiera y no financiera para preservar el valor generado por el gobierno corporativo y sus inversiones. Tomando en cuenta lo anterior este estudio se enfocará sobre las normativas fundamentales que logran cumplir los objetivos de una auditoria en TI.

El presente trabajo consiste en analizar los sistemas de controles la información financiera y no financiera, con un enfoque metodológico cualitativo, basados en marcos de referencia internacionales, los cuales son COBIT 5.0 (Objetivos de Control para la Información y Tecnologías Relacionadas), y según la norma internacional de trabajos de aseguramiento NITA 3402 sobre “informes de atestiguamiento sobre los controles de una organización de servicios” aplicados en la entidad NP Enterprise Inc. proporcionando así un marco integral que ayuda a lograr sus metas y agregar valor mediante un gobierno y una administración efectivos de las TI de la organización.

En conclusión, al tener en cuenta estos marcos normativos se podrá evaluar el cumplimiento de controles específicos en el proceso de auditoría en TI, con la finalidad de proveer al gobierno corporativo información adecuada y útil para la toma de decisiones con el fin de lograr los objetivos enmarcados en la visión planteada de la organización.

v. Índice

Br. Héctor Salgado Palacios
Br. Michael Tejeda Valenzuela

Br. Héctor Salgado Palacios
Br. Michael Tejeda Valenzuela

Br. Héctor Salgado Palacios
Br. Michael Tejeda Valenzuela

I. Introducción al tema y al sub tema

La Informática en la actualidad, está intensamente vinculada en la gestión integral de las organizaciones, por eso las normas y estándares deben estar sometidos a los estándares generales de la misma. En consecuencia, los Sistemas Informáticos se han constituido en las herramientas más poderosas para materializar un sin número de beneficios económicos y estratégicos necesarios para una entidad. La auditoría de tecnologías de la información (TI), son parte importante en el proceso de prevención, mitigación y gestión de riesgos. Las TI deben ser consideradas igual de importantes para el gobierno corporativo, ya que de esta depende el manejo de toda la información financiera que recopila la entidad y depende del buen funcionamiento de estas la confiabilidad en la razonabilidad de las cifras financieras que arrojen los estados financieros, brindando así una oportuna respuesta ante posibles riesgos que pueda tener la entidad, brindando un mejor manejo del control interno.

Se expondrá en este trabajo de seminario de graduación 6 acápites, donde el primer acápite consta de la introducción al tema y sub tema, en el segundo acápite la justificación del mismo, en el tercer acápite están planteados los objetivos que persigue este trabajo, en el cuarto acápite desarrollaremos los aspectos fundamentales de la auditoría en TI, los principios de control que brindan los marcos normativos de carácter internacional como COBIT 5.0 y la NITA 3402; en el quinto acápite mediante un caso práctico se ejemplificará lo ya descrito en el informe ejecutivo, en el sexto acápite se brindaran las conclusiones del trabajo, en el séptimo acápite se destacará la bibliografía utilizada en la elaboración de este documento y en el octavo acápite estarán los anexos del trabajo, documentos que fueron utilizados para la elaboración de este trabajo.

Br. Héctor Salgado Palacios
Br. Michael Tejeda Valenzuela

II. Justificación

La presente investigación tiene como objeto la ejecución de una auditoría de las tecnologías de la información, analizando la estructura de los sistemas de controles en que se basan la creación e implementación de los softwares contables de entidades con el propósito de prevenir y mitigar los riesgos que se presentan y ayudar a la toma de decisiones del gobierno corporativo y las partes interesadas usuarias de la información financiera.

Esta investigación será útil para toda la comunidad de los profesionales de la contabilidad, debido en que en esta se exponen los criterios claves para la realización de una auditoria en TI, basado en marcos normativos internacionales aplicables, como lo son el COBIT 5.0 y las NIA´S.

Debido a que es un trabajo no convencional, y que por lo general solamente se realizan por encargos específicos, la mayoría de los profesionales de la contabilidad tienen pocos conocimientos sobre esta materia, siendo esta primordial en la actualidad producto de la globalización que sufren los sistemas y marcos normativos internacionales que fungen como base en la estructuración de los procesos sistematizados de la información financiera y no financiera que se utiliza para la gestión del gobierno corporativo.

III. Objetivos

3.1 Objetivo General

3.1.1 Analizar el sistema de control interno de la Tecnología de la Información de NP Enterprise Inc. utilizado para garantizar la veracidad, confidencialidad, confiabilidad y disponibilidad de la información financiera y no financiera al 31 de diciembre 2016 mediante la aplicación de COBIT 5.0 y según la Norma Internacional de Trabajos de Aseguramiento NITA 3402.

3.2 Objetivos Específicos

3.2.1. Enunciar los aspectos fundamentales de la auditoría en T.I.

3.2.2. Describir el proceso que debe de llevar a cabo una organización para el buen gobierno corporativo según COBIT 5.0 en cuanto a control interno de TI.

3.2.3. Mencionar el marco normativo internacional que atañe a la auditoría de T.I. (ISAE 3402).

3.2.4. Desarrollar mediante un caso práctico el análisis sobre los controles de la información financiera y no financiera aplicando los marcos normativos COBIT 5.0 y NITA 3402.

IV. Desarrollo del sub tema

4.1. Auditoría de Tecnologías de la información

La auditoría es un examen que se realiza con carácter objetivo, crítico, sistemático y selectivo con el fin de evaluar la eficacia y eficiencia del uso adecuado de los recursos informáticos, de la gestión informática y si estas han brindado el soporte adecuado a los objetivos y metas del negocio. (Hernández Salguera, 2011). Párr. 7.

(Arens, Elder, & Beasley, 2007). La Auditoría es la acumulación y evaluación de la evidencia basada en información para determinar y reportar sobre el grado de correspondencia entre la información y los criterios establecidos. La auditoría debe realizarla una persona independiente y competente. Párr. 8.

La tecnología de la información (TI, o más conocida como IT por su significado en inglés: information technology) es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras empresas. (Arens, Elder, & Beasley, 2007). Párr. 1.

4.1.1. Auditoría de tecnologías de la información: una pieza clave

La informática hoy está sumida en la gestión integral de la empresa, y por eso las normas estándares propiamente informáticos deben estar, por lo tanto, sometidos a los generales de la misma.

Br. Héctor Salgado Palacios
Br. Michael Tejeda Valenzuela

Las organizaciones informáticas forman parte de lo que se ha denominado el "management" o gestión de la empresa debido a su importancia en el funcionamiento de una empresa, existe la auditoría informática. (Hernández Salguera, 2011). Párr. 11-12.

La auditoría de tecnología de la información (T.I) como se le conoce actualmente, (Auditoría informática de sistemas en nuestro medio), se ha consolidado en el mundo entero como cuerpo de conocimientos cierto y consistente, respondiendo a la acelerada evolución de la tecnología informática de los últimos 10 años.

La información es considerada un activo tan o más importante que cualquier otro en una organización. (Hernández Salguera, 2011). Párr. 15-16.

Existe pues, un cuerpo de conocimientos, normas, técnicas y buenas prácticas dedicadas a la evaluación y aseguramiento de la calidad, seguridad, razonabilidad y disponibilidad de la información tratada y almacenada a través de un computador y equipos afines, así como de la eficiencia, eficacia y economía con que la administración de un ente están manejando dicha información y todos los recursos físicos y humanos asociados para su adquisición, captura, procesamiento, transmisión, distribución, uso y almacenamiento. Todo lo anterior con el objetivo de emitir una opinión o juicio, para lo cual se aplican técnicas de auditoria de general aceptación y conocimiento técnico específico. (Hernández Salguera, 2011) Párr. 19.

4.1.2. Objetivos de la auditoría Informática

La auditoría informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

Esta es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además, debe evaluar todo: informática, organización de centros de información. (Hernández Salguera, 2011). Párr. 21-22.

4.1.3. Alcance de la auditoría informática

El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoría informática, se complementa con los objetivos de ésta.

El alcance ha de figurar expresamente en el informe final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas. (Hernández Salguera, 2011). Párr. 30-31.

4.1.4. Características de la auditoría informática

La información financiera de la empresa y para la empresa, siempre importante, se ha convertido en un activo real de la misma, como sus stocks o materias primas si las hay. Por ende, han de realizarse inversiones informáticas, materia de la que se ocupa la auditoría de inversión informática.

Del mismo modo, los sistemas informáticos han de protegerse de modo global y particular: a ello se debe la existencia de la auditoría de seguridad informática en general, o a la auditoría de seguridad de alguna de sus áreas como pudieran ser desarrollo o técnica de sistemas.

Cuando se producen cambios estructurales en la Informática, se reorganiza de alguna forma su función: se está en el campo de la Auditoría de Organización Informática.

Estos tres tipos de auditorías engloban a las actividades auditoras que se realizan en una auditoría parcial. De otra manera: cuando se realiza una auditoria del área de Desarrollo de Proyectos de la Informática de una empresa, es porque en ese Desarrollo existen, además de ineficiencias, debilidades de organización, o de inversiones, o de seguridad, o alguna mezcla de ellas. (Hernández Salguera, 2011). Párr. 39-42.

4.1.5. Herramientas y técnicas para la auditoría en TI

Las técnicas son los procedimientos que se usan en el desarrollo de un proyecto de auditoría informática, algunas de las más comunes son:

- Análisis y diseño estructurado.
- Graficas de Pert.
- Graficas de Gantt.
- Documentación.
- Programación estructurada.
- Modulación de datos y procesos.

Las herramientas son el conjunto de elementos que permiten llevar a cabo las acciones definidas en las técnicas. Las herramientas utilizadas son:

- Cuestionarios.
- Entrevistas.
- Checklist.
- Trazabilidad de la información. (Hernández Salguera, 2011). Párr.90-91.

4.1.5.1. Cuestionarios

Son el conjunto de preguntas a las que el sujeto puede responder oralmente o por escrito, cuyo fin es poner en evidencia determinados aspectos.

Ya que las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma. (Hernández Salguera, 2011). Párr. 92-94.

4.1.5.2. Entrevistas

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información y mejor descrita que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas, también sencillas. (Hernández Salguera, 2011). Párr.95-96.

4.1.5.3. Checklist

El auditor profesional y experto es aquel que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para la cumplimentación sistemática de sus cuestionarios, de sus checklist. (Hernández Salguera, 2011). Párr. 97.

4.1.5.4. Trazabilidad de la información

Con frecuencia, el auditor informático debe verificar que los programas, tanto de los sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en productos software muy potentes y modulares que siguen los datos a través del programa.

La trazabilidad se utiliza para comprobar la ejecución de las validaciones de datos previstas. La trazabilidad en si no debe modificar en absoluto el sistema. (Hernández Salguera, 2011). Párr. 99-100.

4.1.6. Riesgos de la información

(Hernández Salguera, 2011). Riesgo es todo tipo de vulnerabilidades y amenazas en cuanto a la seguridad de la información que pueden ocurrir y producir numerosas pérdidas para las empresas. Párr. 130.

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la veracidad, confidencialidad, confiabilidad y disponibilidad de la misma. (Hernández Salguera, 2011). Párr.131.

4.1.6.1. Importancia de la información

Se suele pasar por alto la base que hace posible la existencia de los anteriores elementos. Esta base es la información.

En el mundo actual, esto está conformado por las Empresas y Compañías, que tienen una organización en particular que permite definir distintas áreas de Trabajo en las que se dividen las tareas de acuerdo a especializaciones, teniendo los distintos empleados un rol en particular dependiendo no solo de su Formación Profesional, sino también de su eficiencia para lo cual han sido contratados.

Por lo que la importancia de la información radica en cuatro factores:

- Esta almacenada y procesada en computadoras.
- Puede ser confidencial para algunas personas o a escala institucional.
- Puede ser mal utilizada o divulgada.
- Puede estar sujeta a robos, sabotaje o fraudes.

En la actualidad gracias a la infinidad de posibilidades que se tiene para tener acceso a los recursos de manera remota y al gran incremento en las conexiones a la internet los delitos en el ámbito de TI se han visto incrementados, bajo estas circunstancias los riesgos son más latentes.

Dentro de ellos se detallan los más importantes:

- Fraudes.
- Falsificación.
- Venta de información.
- Destrucción de la información. (Arens, Elder, & Beasley, 2007). Párr. 14-19.

4.1.6.2. El manejo de riesgos de la información

Manejo de riesgo, un concepto durante mucho tiempo usado en toma de decisiones que se toman en conjunto, el manejo de riesgo es un esfuerzo coordinado para proteger los bienes financieros, físicos y humanos de la organización.

Dentro del manejo de riesgos de la seguridad en la información se estudian distintos factores.

- Evitar

No se permite ningún tipo de exposición. Esto se logra simplemente con no comprometerse a realizar la acción que origine el riesgo. Esta técnica tiene más desventajas que ventajas, ya que la empresa podría abstenerse de aprovechar muchas oportunidades.

- Reducir

Cuando el riesgo no puede evitarse por tener varias dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más bajo posible. Esta opción es la más económica y sencilla. Se consigue optimizando los procedimientos la implementación controles y su monitoreo constante.

- Retener, asumir o aceptar el riesgo

Aceptar las consecuencias de la ocurrencia del evento, puede ser voluntaria o involuntaria, la voluntaria se caracteriza por el reconocimiento de la existencia del riesgo y el acuerdo de asumir las pérdidas involucradas, esta decisión se da por falta de alternativas. La retención involuntaria se da cuando el riesgo es retenido inconscientemente.

- Transferir

Es buscar un respaldo y compartir el riesgo con otros controles o entidades. Esta técnica se usa ya sea para eliminar un riesgo de un lugar y transferir a otro, o para minimizar el mismo, compartiendo con otras entidades. (Arens, Elder, & Beasley, 2007). Párr. 20-26.

4.1.6.3. Factores de riesgo de la información

La amplia variedad de amenazas que afectan a los equipos de información siempre se cristaliza en una única consecuencia: el sistema deja de funcionar.

- factores físicos: en ellos se encuentra el cableado, la iluminación, el aire de renovación o ventilado y las fuentes de alimentación.
- Factores ambientales: en estos se encuentran los incendios, inundaciones, sismos y la humedad,
- Factores humanos: dentro de ellos los robos, actos vandálicos, actos vandálicos contra el sistema de red, fraude, sabotaje, terrorismo. (Arens, Elder, & Beasley, 2007). Párr. 30-31.

4.1.7. Control interno informático

El control interno como cualquier actividad o acción realizada manual o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos.

El informe COSO define el control interno como las normas, los procedimientos, las prácticas y las estructuras organizativas diseñadas para proporcionar seguridad razonable de que los objetivos de la empresa se alcanzarán y que los eventos no deseados se preverán, se detectarán y se corregirán.

En el ambiente informático, el control interno se materializa fundamentalmente en controles de dos tipos.

- Controles manuales: aquellos que son ejecutados por el personal del área usuaria o de informática sin la utilización de herramientas computacionales.
- Controles automáticos; son generalmente los incorporados en el software, llámense estos de operación, de comunicación, de gestión de base de datos, programas de aplicación, etc. Véase reflejado en la siguiente figura. (Arens, Elder, & Beasley, 2007). Párr. 30-34.

4.1.7.1. Principales objetivos

- Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- Asesorar sobre el conocimiento de las normas.

- Colaborar y apoyar el trabajo de auditoria informática interna/ externa
- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informático. (Arens, Elder, & Beasley, 2007). Párr. 52.

4.1.7.2. Funciones específicas

- Difundir y controlar el cumplimiento de las normas, estándares y procedimientos al personal de programadores, técnicos y operadores.
- Diseñar la estructura del sistema de control interno de la dirección de informática en los siguientes aspectos.
- Desarrollo y mantenimiento del software de aplicación.
- Explotación de servicios principales.
- Software de base
- Redes de computación
- Seguridad informática
- Licencias de software
- Cultura de riesgo informático en la organización
- Control informático. (áreas de aplicación). (Arens, Elder, & Beasley, 2007). Párr. 49

4.1.7.3. Clasificación de los controles internos informáticos

El sistema de control interno es un sistema integrado al proceso administrativo, en la planeación, organización, dirección y control de las operaciones con el objeto de asegurar la protección de todos los recursos informáticos y mejorar los índices de economía, eficiencia y efectividad de los procesos operativos automatizados, los controles internos se clasifican de la siguiente manera:

- Controles preventivos: sirve para tratar de evitar un evento no deseado de todas las áreas de departamento como son: equipo de cómputo, sistemas, telecomunicaciones.
- Controles detectivos: trata de descubrir a posteriori errores o fraudes que no haya sido posible evitarlos con controles preventivos.
- Controles correctivos: tratan de asegurar que se subsanen todos los errores identificados, mediante los controles preventivos, es decir facilitan la vuelta a la normalidad ante una incidencia. Es un plan de contingencia. (Arens, Elder, & Beasley, 2007). Párr. 54.

4.2. COBIT 5.0, un marco de negocios para el gobierno y la gestión de los TI de la empresa.

COBIT 5 ayuda a las Organizaciones a crear un valor óptimo a partir de la TI, al mantener un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos.

COBIT 5 permite que las tecnologías de la información y relacionadas se gobiernen y administren de una manera holística a nivel de toda la Organización, incluyendo el alcance completo de todas las áreas de responsabilidad funcionales y de negocios, considerando los

intereses relacionados con la TI de las partes interesadas internas y externas. (ISACA, 2012). Párr. 10-11.

4.2.1. Definición.

COBIT 5 une los cinco principios que permiten a la Organización construir un marco efectivo de Gobierno y Administración basado en una serie holística de siete habilitadores, que optimizan la inversión en tecnología e información, así como su uso en beneficio de las partes interesadas.

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público. (ISACA, 2012). Párr. 10-12.

4.2.2. Principios del COBIT 5

COBIT 5 se basa en cinco principios claves para el gobierno y la gestión de las TI empresariales, véase en la figura 2. Principios COBIT 5.

Figura 2: Principios de COBIT 5.0

Fuente: (ISACA, 2012)

4.2.2.1. Satisfacer las necesidades de las partes interesadas.

Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos. COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI. Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar COBIT 5 para adaptarlo a su propio contexto mediante la cascada de metas, traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos. Véase en la figura 3. (ISACA, 2012). Párr. 14.

Figura 3: Necesidades de las partes interesadas

Fuente: (ISACA, 2012)

Las empresas tienen muchas partes interesadas, y 'crear valor' significa cosas diferentes y a veces contradictorias para cada uno de ellos. Las actividades de gobierno tratan sobre negociar y decidir entre los diferentes intereses en el valor de las partes interesadas. En consecuencia, el sistema de gobierno debe considerar a todas las partes interesadas al tomar decisiones sobre beneficios, evaluación de riesgos y recursos. Para cada decisión, las siguientes preguntas pueden y deben hacerse: ¿Para quién son los beneficios? ¿Quién asume el riesgo? ¿Qué recursos se requieren? (ISACA, 2012). Párr. 16.

Cada empresa opera en un contexto diferente; este contexto está determinado por factores externos (el mercado, la industria, geopolítica, etc.) y factores internos (la cultura, organización, umbral de riesgo, etc.) y requiere un sistema de gobierno y gestión personalizado.

Las necesidades de las partes interesadas deben transformarse en una estrategia corporativa factible. La cascada de metas de COBIT 5 es el mecanismo para traducir las necesidades de las partes interesadas en metas corporativas, metas relacionadas con las TI y metas catalizadoras específicas, útiles y a medida. Esta traducción permite establecer metas

específicas en todos los niveles y en todas las áreas de la empresa en apoyo de los objetivos generales y requisitos de las partes interesadas y así, efectivamente, soportar la alineación entre las necesidades de la empresa y las soluciones y servicios de TI. (ISACA, 2012). Párr. 18-19.

Para ello se muestra la cascada de metas de COBIT 5.

Paso 1. Los Motivos de las Partes Interesadas Influyen en las Necesidades de las Partes Interesadas. Las necesidades de las partes interesadas están influenciadas por diferentes motivos, por ejemplo, cambios de estrategia, un negocio y entorno regulatorio cambiantes y las nuevas tecnologías.

Paso 2. Las Necesidades de las Partes Interesadas Desencadenan Metas Empresariales. Las necesidades de las partes interesadas pueden estar relacionadas con un conjunto de metas empresariales genéricas. Estas metas corporativas han sido desarrolladas utilizando las dimensiones del cuadro de mando integral (CMI. En inglés: Balanced Scorecard, BSC)1 y representan una lista de objetivos comúnmente usados que una empresa puede definir por sí misma. Aunque esta lista no es exhaustiva, la mayoría metas corporativas específicas de la empresa pueden relacionarse fácilmente con uno o más de los objetivos genéricos de la empresa. En el Apéndice D se representa una tabla de las partes interesadas y metas corporativas.

Paso 3. Cascada de Metas de Empresa a Metas Relacionadas con las TI. El logro de metas empresariales requiere un número de resultados relacionados con las TI2, que están representados por las metas relacionadas con la TI. Se entiende como relacionados con las TI a la información y tecnologías relacionadas, y las metas relacionadas con las TI se estructuran en dimensiones del CMI. COBIT 5 define 17 metas relacionadas con las TI.

Paso 4. Cascada de Metas Relacionadas con las TI Hacia Metas Catalizadoras. Alcanzar metas relacionadas con las TI requiere la aplicación satisfactoria y el uso de varios catalizadores. Los catalizadores incluyen procesos, estructuras organizativas e información, y para cada catalizador puede definirse un conjunto de metas relevantes en apoyo de las metas relacionadas con la TI. véase el ejemplo en la figura 4. (ISACA, 2012). Párr. 17-22.

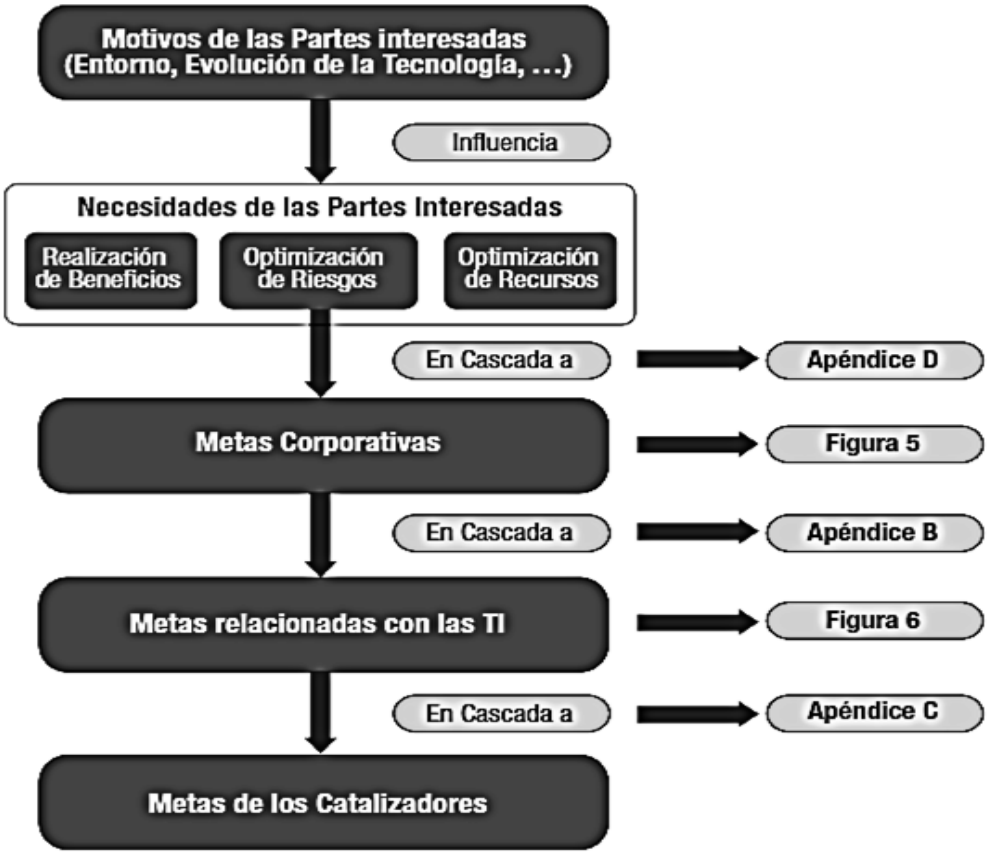


Figura 4: Cascada de metas de COBIT 5

Fuente: (ISACA, 2012)

4.2.2.2. Cubrir la empresa de extremo a extremo.

COBIT 5 contempla el gobierno y la gestión de la información y la tecnología relacionada desde una perspectiva extremo a extremo y para toda la empresa.

Eso significa que Integra el gobierno de la empresa TI en el gobierno corporativo. Es decir, el sistema de gobierno para la empresa TI propuesto por COBIT 5 se integra sin problemas en cualquier sistema de gobierno. COBIT 5 se alinea con las últimas visiones sobre gobierno.

Cubre todas las funciones y procesos necesarios para gobernar y gestionar la información corporativa y las tecnologías relacionadas donde quiera que esa información pueda ser procesada. Dado este alcance corporativo amplio, COBIT 5 contempla todos los servicios TI internos y externos relevantes, así como los procesos de negocio internos y externos. (ISACA, 2012). Párr. 30-32.

COBIT 5 proporciona una visión integral y sistémica del gobierno y la gestión de la empresa TI (ver el principio 4), basada en varios catalizadores. Los catalizadores son para toda la empresa y extremo-a-extremo, es decir, incluyendo todo y a todos, internos y externos, que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionada, incluyendo las actividades y responsabilidades tanto de las funciones TI como de las funciones de negocio.

La información es una de las categorías de catalizadores de COBIT. El modelo mediante el que COBIT 5 define los catalizadores permite a cada grupo de interés definir requisitos exhaustivos y completos para la información y el ciclo de vida de procesamiento de la información, conectando de este modo el negocio y su necesidad de una información adecuada y la función TI, y soportando el negocio y el enfoque de contexto.

(ISACA, 2012). El enfoque de gobierno extremo a extremo que es la base de COBIT 5 está representado en la figura 5, mostrando los componentes clave de un sistema de gobierno. Párr. 34-36.

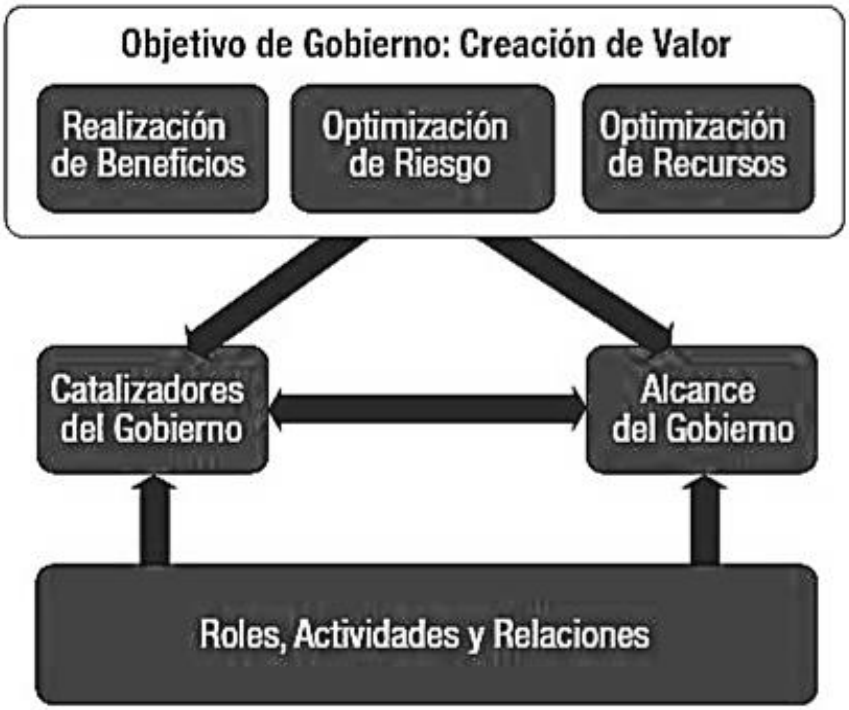


Figura 5 Gobierno y gestión en COBIT 5

Fuente: (ISACA, 2012)

4.2.2.3. Aplicar un marco de referencia único integrado

COBIT 5 es un marco de referencia único e integrado porque:

- Se alinea con otros estándares y marcos de referencia relevantes y, por tanto, permite a la empresa usar COBIT 5 como el marco integrador general de gestión y gobierno.
- Es completo en cuanto a la cobertura de la empresa, proporcionando una base para integrar de manera efectiva otros marcos, estándares y prácticas utilizadas. Un marco general único sirve como una fuente consistente e integrada de guía en un lenguaje común, no-técnico y tecnológicamente agnóstico.
- Proporciona una arquitectura simple para estructurar los materiales de guía y producir un conjunto consistente.

- Integra todo el conocimiento disperso previamente en los diferentes marcos de ISACA. ISACA ha investigado las áreas clave del gobierno corporativo durante muchos años y ha desarrollado marcos tales como COBIT, Val IT, Risk IT, BMIS, la publicación Información sobre Gobierno de TI para la Dirección (Board Briefing on IT Governance) e ITAF para proporcionar guía y asistencia a las empresas. COBIT 5 integra todo este conocimiento.
- La investigación y utilización de un conjunto de fuentes que han impulsado el nuevo contenido desarrollado, incluyendo: la unión de todas las guías existentes de ISACA (COBIT4.1, Val IT 2.0, Risk IT, BMIS) en este único marco.
- Completar este contenido con áreas que necesitaban más elaboración y actualización.
- El alineamiento a otros estándares y marcos relevantes, tales como ITIL, TOGAF y estándares ISO.
- Se puede encontrar una lista completa de referencias en el Apéndice A Definiendo un conjunto de catalizadores de gobierno y gestión que proporcionan una estructura para todos los materiales de guía. Poblando una base de conocimiento COBIT 5 que contiene todas las guías y contenido producido hasta ahora y que proporcionará una estructura para contenidos futuros adicionales. Proporcionando una referencia base de buenas prácticas exhaustiva y sólida.
- (ISACA, 2012). El marco de referencia COBIT 5 proporciona a sus grupos de interés la guía más completa y actualizada, ver figura 6 sobre el gobierno y la gestión de la empresa TI. Párr. 37-44.

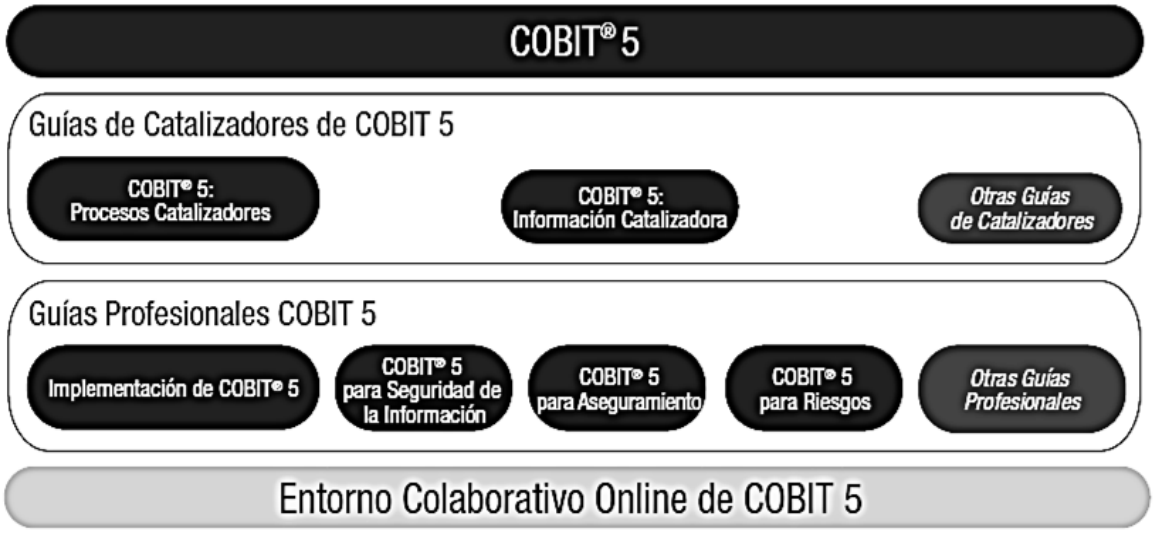


Figura 6: Familia de productos COBIT 5

Fuente: (ISACA, 2012)

4.2.2.4. Hacer un posible enfoque holístico

Los catalizadores son factores que, individual y colectivamente, influyen sobre si algo funcionará en este caso, el gobierno y la gestión de la empresa TI. Los catalizadores son guiados por la cascada de metas, es decir, objetivos de alto nivel relacionados con TI definen lo que los diferentes catalizadores deberían conseguir.

El marco de referencia COBIT 5 describe siete categorías de catalizadores:

- Principios, políticas y marcos de referencia son el vehículo para traducir el comportamiento deseado en guías prácticas para la gestión del día a día.
- Los procesos describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de resultados que soporten las metas generales relacionadas con TI.
- Las estructuras organizativas son las entidades de toma de decisiones clave en una organización.

- La Cultura, ética y comportamiento de los individuos y de la empresa son muy a menudo subestimados como factor de éxito en las actividades de gobierno y gestión.
- La información impregna toda la organización e incluye toda la información producida y utilizada por la empresa. La información es necesaria para mantener la organización funcionando y bien gobernada, pero a nivel operativo, la información es muy a menudo el producto clave de la empresa en sí misma.
- Los servicios, infraestructuras y aplicaciones incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.
- Las personas, habilidades y competencias están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y de acciones correctivas, ver la figura 7. (ISACA, 2012). Párr. 50-55.

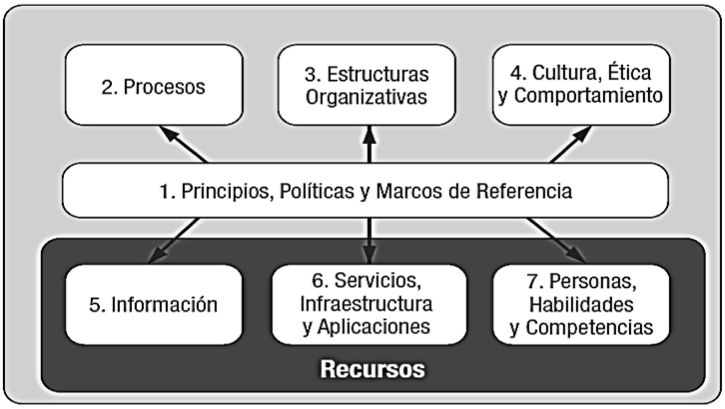


Figura 7: Catalizadores corporativos

Fuente: (ISACA, 2012)

Algunos de los catalizadores definidos previamente son también recursos corporativos que también necesitan ser gestionados y gobernados. Esto aplica a:

- La información, que necesita ser gestionada como un recurso. Alguna información, tal como informes de gestión y de inteligencia de negocio son importantes catalizadores para el gobierno y la gestión de la empresa.
- Servicios, infraestructura y aplicaciones.
- Personas, habilidades y competencias. (ISACA, 2012). Párr. 58.

4.2.2.5. Separa al gobierno de la gestión.

El marco de COBIT 5 realiza una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren estructuras organizativas diferentes y sirven para diferentes propósitos.

La posición de COBIT 5 sobre esta fundamental distinción entre gobierno y gestión es:

- Gobierno: asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.
- Gestión: La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

Partiendo de las definiciones entre gobierno y gestión, está claro que comprenden diferentes tipos de actividades, con diferentes responsabilidades; sin embargo, dado el papel de gobierno evaluar, orientar y vigilar se requiere un conjunto de interacciones entre gobierno y

gestión para obtener un sistema de gobierno eficiente y eficaz. Estas interacciones, empleando una estructura de catalizadores.

Asimismo, el modelo de referencia de procesos de COBIT 5, no es prescriptivo, pero sí defiende que las empresas implementen procesos de gobierno y de gestión de manera que las áreas fundamentales estén cubiertas, tal y como se muestra en la figura 8. (ISACA, 2012). Párr. 60-63.

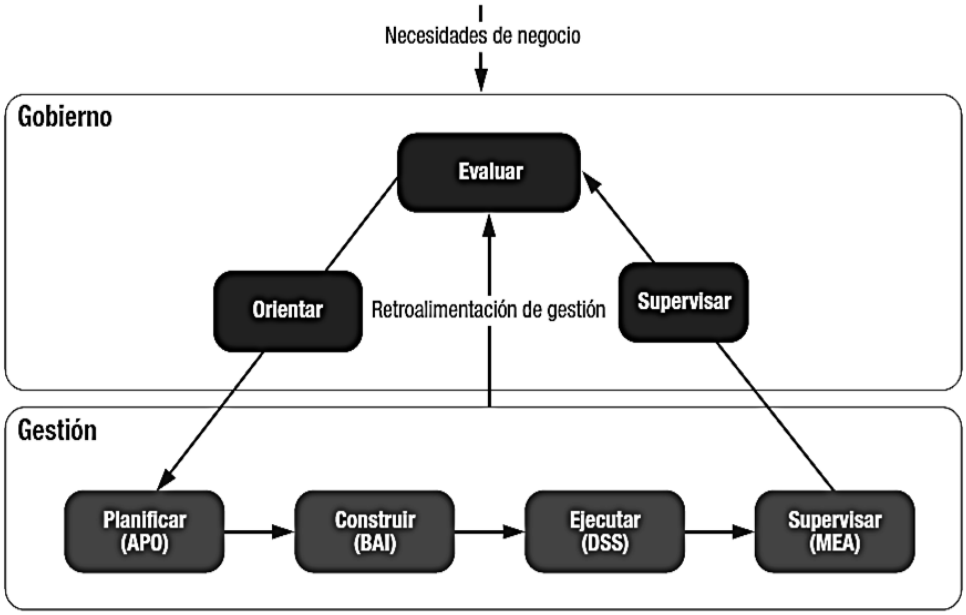


Figura 8: Las áreas claves de gobierno y gestión de COBIT 5

Fuente: (ISACA, 2012)

Una empresa puede organizar sus procesos como crea conveniente, siempre y cuando las metas de gobierno y gestión queden cubiertas. Empresas más pequeñas pueden tener pocos procesos; empresas más grandes y complejas pueden tener numerosos procesos, pero todos con el ánimo de cubrir las mismas metas.

COBIT 5 incluye un modelo de referencia de procesos que define y describe en detalle varios procesos de gobierno y de gestión. Dicho modelo representa todos los procesos que normalmente encontramos en una empresa relacionados con las actividades de TI, proporciona

un modelo de referencia común entendible para las operaciones de TI y los responsables de negocio. El modelo de proceso propuesto es un modelo completo e integral, pero no constituye el único modelo de procesos posible. Cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación particular.

La incorporación de un modelo operacional y un lenguaje común para todas las partes de la empresa involucradas en las actividades de TI es uno de los pasos más importantes y críticos hacia el buen gobierno. Adicionalmente proporciona un marco para medir y vigilar el rendimiento de TI, proporcionar garantía de TI, comunicarse con los proveedores de servicio e integrar las mejores prácticas de gestión.

El modelo de referencia de procesos de COBIT 5 divide los procesos de gobierno y de gestión de la TI empresarial en dos dominios principales de procesos:

- Gobierno: contiene cinco procesos de gobierno; dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión (EDM).
- Gestión: contiene cuatro dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar.

Estos dominios son una evolución de la estructura de procesos y dominios de COBIT 4.1. Los nombres de estos dominios han sido elegidos de acuerdo a estas designaciones de áreas principales, pero contienen más verbos para describirlos:

- Alinear, Planificar y Organizar (Align, Plan and Organise, APO)
- Construir, Adquirir e Implementer (Build, Acquire and Implement, BAI)
- Entregar, dar Servicio y Soporte (Deliver, Service and Support, DSS)
- Supervisar, Evaluar y Valorar (Monitor, Evaluate and Assess, MEA)

- y supervisar (Plan, Build, Run and Monitor - PBRM), y proporciona cobertura de extremo a extremo de las TI

Cada dominio contiene un número de procesos. A pesar de que, según hemos descrito antes, la mayoría de los procesos requieren de actividades de “planificación”, “implementación”, “ejecución” y “supervisión”, bien en el propio proceso, o bien en la cuestión específica a resolver (como p. ej. calidad, seguridad), están situados en dominios de acuerdo con el área más relevante de actividad cuando se considera la TI a un nivel empresarial.

El modelo de referencia de procesos de COBIT 5 es el sucesor del modelo de procesos de COBIT 4.1 e integra también los modelos de procesos de Risk IT y Val IT.

(ISACA, 2012). La figura 9 muestra el conjunto completo de los 37 procesos de gobierno y gestión de COBIT 5. Los detalles de todos los procesos, de acuerdo con el modelo de proceso anteriormente descrito, están recogidos en la guía *COBIT 5:* Procesos Catalizadores. Párr. 65-70.

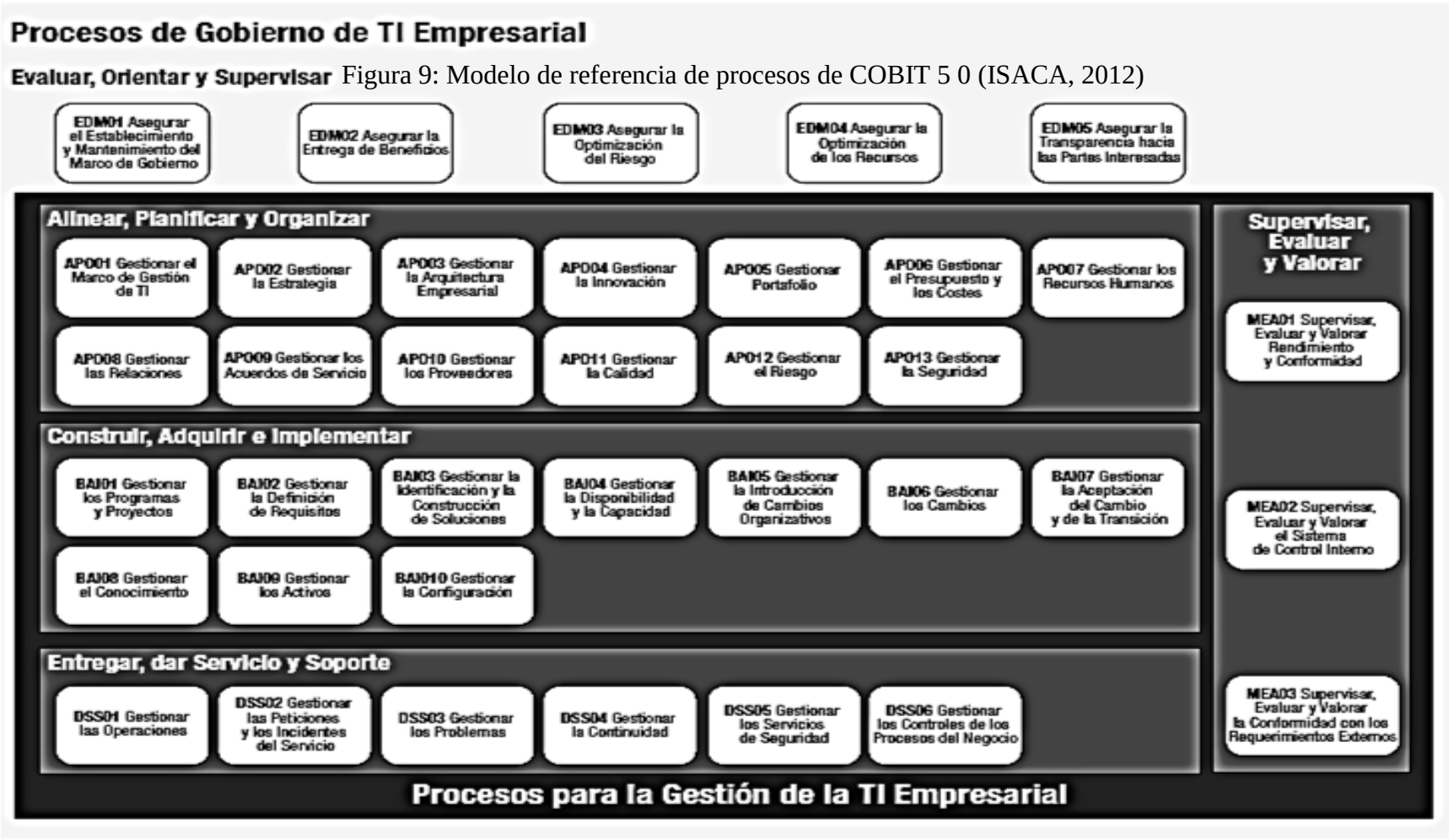


Figura 9: Modelo de referencia de procesos de COBIT 5 0 (ISACA, 2012)

Figura 9: Procesos Catalizadores COBIT 5.0

Fuente: (ISACA, 2012)

4.2.3. Guía de implantación

Podemos obtener un valor óptimo aprovechando COBIT solo si es adoptado y adaptado de manera eficaz para ajustarse al entorno único de cada empresa. Cada enfoque de implementación también necesitará resolver desafíos específicos, incluyendo la gestión de cambios a la cultura y el comportamiento.

ISACA proporciona amplias y prácticas guías de implementación en su publicación COBIT 5 Implementación, que está basada en un ciclo de vida de mejora continua. No está pensada con un enfoque prescriptivo ni como una solución completa, sino más bien como una guía para evitar los obstáculos más comunes, aprovechar las mejores prácticas y ayudar en la creación de resultados satisfactorios. La guía se complementa con una herramienta de implementación que contiene varios recursos que serán mejorados continuamente. Sus contenidos incluyen:

- Herramientas de autoevaluación, medición y diagnóstico
- Presentaciones orientadas a diversas audiencias
- Artículos relacionados y explicaciones adicionales

El propósito de este capítulo es presentar el ciclo de vida de la implementación y mejora continua, desde un punto de vista de alto nivel y destacar una serie de aspectos importantes de *COBIT 5* Implementación, como, por ejemplo:

- Realizar un caso de negocio para la implementación y mejora del gobierno y gestión de TI.
- Reconocer los típicos puntos débiles y eventos desencadenantes
- Crear el entorno apropiado para la implementación

- Aprovechar COBIT para identificar carencias y guiar en el desarrollo de elementos facilitadores como políticas, procesos, principios, estructuras organizativas y roles y responsabilidades.

El gobierno y la gestión de la TI empresarial no suceden de manera aislada. Cada empresa necesita diseñar su propio plan de implantación, atendiendo a los factores específicos del entorno interno y externo de la empresa, como, por ejemplo:

- Ética y cultura
- Leyes aplicables, regulaciones y políticas
- Misión, visión y valores
- Políticas y prácticas de gobierno
- Plan de negocio y perspectivas estratégicas
- Modelo operativo y nivel de madurez
- Estilo de gestión
- Umbral de riesgo
- Capacidades y recursos disponibles
- Prácticas de la industria

El enfoque óptimo para el gobierno y gestión de la TI empresarial será distinto para cada empresa, siendo necesario entender y considerar el contexto para adoptar y adaptar COBIT de modo efectivo en la implementación de los catalizadores de gobierno y gestión de TI empresarial. COBIT es a menudo complementado por otros marcos, buenas prácticas y estándares, y éstos también necesitan ser adaptados para ajustarse a los requisitos específicos.

Algunos factores críticos de éxito para una implementación con éxito son:

- Que la alta dirección proporcione la orientación y directrices para la iniciativa, así como un decidido compromiso y apoyo.
- Todas las partes deben apoyar los procesos de gobierno y gestión, para entender el negocio y las metas de TI.
- Asegurar la comunicación efectiva y la habilitación de los cambios necesarios.
- Personalizar COBIT y otras buenas prácticas y estándares empleados para ajustarlos al entorno único de la empresa.
- Enfocarse en resultados inmediatos (quick wins) y priorizar las mejoras más beneficiosas que sean más sencillas de implementar. (ISACA, 2012). Párr. 75-83.

4.2.3.1. Creando el entorno apropiado

Es importante para las iniciativas de implementación que se apoyen en COBIT que sean correctamente gobernadas y adecuadamente gestionadas. La mayoría de las iniciativas relacionadas con TI fracasan a menudo por una dirección, soporte y supervisión inadecuados por las distintas partes interesadas necesarias, y la implementación de herramientas de gobierno o gestión de TI que se apoyan en COBIT no es diferente. El apoyo y orientación de las partes interesadas clave es crítico para que las mejoras sean adoptadas y mantenidas. En un entorno empresarial de poca fortaleza (como, por ejemplo, un modelo operativo de negocio poco claro o carente de catalizadores de gobernabilidad a nivel empresarial), este apoyo y participación es todavía más importante.

Los catalizadores que aprovecha COBIT deberían proporcionar una solución considerando necesidades y problemas reales de negocio en lugar de ser un fin en sí mismos. Los requerimientos basados en aspectos sensibles y factores actuales deberían ser identificados por la dirección como áreas que tienen que ser consideradas. Las comprobaciones de alto nivel, los diagnósticos y las valoraciones basadas en COBIT son excelentes herramientas para concienciar, crear consenso y generar compromiso para actuar. Desde el inicio se debe solicitar el compromiso e interiorización de las partes interesadas más relevantes. Para conseguir esto, los objetivos y beneficios de la implementación necesitan ser claramente expresados en términos de negocio y resumidos en un resumen de caso de negocio.

Una vez que el compromiso ha sido obtenido, es necesario contar con los recursos adecuados para apoyar el programa. Los roles y responsabilidades esenciales del programa deberían ser definidos y asignados. Hay que tener cuidado de cara al exterior en mantener el compromiso de todas las partes interesadas afectadas.

Se deberían establecer y mantener las estructuras y procesos apropiados para supervisar y orientar. Estas estructuras y procesos deberían también asegurar la alineación con los enfoques de gobierno corporativo y de gestión del riesgo.

(ISACA, 2012). Tanto las partes interesadas clave como el consejo y los ejecutivos deberían proporcionar apoyo visible y compromiso para establecer el ejemplo de la cúpula empresarial y garantizar el compromiso con el programa a todos los niveles. Párr. 90-95.

4.3. Norma internacional de trabajos de aseguramiento sobre los controles de una organización de servicios NITA 3402.

4.3.1. Alcance

El control interno es un proceso diseñado para ofrecer una seguridad razonable sobre el logro de los objetivos relacionados con la confiabilidad de los informes financieros, la efectividad y la eficiencia de las operaciones y el cumplimiento de la legislación y regulación aplicables. Los controles relacionados con las operaciones de una empresa u organización de servicios y los objetivos de cumplimiento pueden ser importantes para el control interno de una entidad usuaria.

Respecto a la información financiera, estos controles pueden referirse a las aseveraciones sobre la presentación y revelación a saldos de cuenta, clases de transacciones o relevaciones o pueden referirse a la evidencia que el auditor evalúa o utiliza para aplicar los procedimientos de auditoria. Por ejemplo, los controles de una organización que procesa los pagos de nómina, relacionados con el envío oportuno de las deducciones salariales a las autoridades gubernamentales.

Puede ser relevante para una entidad usuaria, en virtud de los envíos inoportunos, pudiera generar o incurrir en intereses y multas para la entidad usuaria. Del mismo modo los controles de una empresa u organización de servicios sobre la aceptabilidad de transacciones de inversión desde la perspectiva normativa, puede considerarse significativo para la presentación y revelación de transacciones y saldos de cuentas de una entidad usuaria en sus estados financieros.

La determinación de si los controles en una empresa u organización de servicio relacionado con las operaciones y su cumplimiento, tiene la posibilidad de ser importante para el control interno de las entidades usuarias en relación con la información financiera en una cuestión de criterio profesional, teniendo en cuenta los objetivos de control establecidos por la empresa u organización de servicios y lo apropiado de los criterios.

La empresa u organización de servicio quizás no pueda afirmar que el sistema está apropiadamente diseñado cuando, por ejemplo, está operando un sistema que fue diseñado por una entidad usuaria o que fue estipulado en un contrato entre una entidad usuaria y la empresa u organización de servicios, debido a la relación intrínseca que existe entre el diseño adecuado de los controles y su efectividad operativa, la ausencia de una aseveración con respecto a lo apropiado del diseño, es probable que impida al auditor concluir que los controles ofrecen una seguridad razonable de que lograron los objetivos de control y por tanto, emitir una opinión sobre la efectividad operativa de los controles.

(International Federación of accountants, 2010). Como alternativa, el profesional puede optar por aceptar un trabajo de procedimiento convenido para probar los controles, o un trabajo de aseguramiento de acuerdo la ISAE 3000, para concluir sobre si, con base en las pruebas de control, esto se ha operado como se describe. Párr. 201-206.

4.3.1.1. Definición.

La definición de controles en la organización de servicios incluye los aspectos de los sistemas de información de las entidades usuarias, administrados por la empresa u organización de servicio, y también pueden incluir los aspectos de uno o más componentes del control interno en tal organización.

Por ejemplo, puede incluir a los aspectos del entorno de control de una empresa u organización de servicio, del monitoreo y actividades de control de los servicios brindados. Sin embargo, no incluye los controles de una empresa u organización de servicios, no están relacionados con el logro de los objetivos de control establecidos en la descripción de sus sistemas, por ejemplo, los controles relacionados con la preparación de los estados financieros propios de la organización

La realización de los procedimientos en la empresa de sub-servicio implica la coordinación y comunicación entre las organizaciones de servicio, la empresa de sub-servicio y el auditor de servicio, por lo general el método de inclusión es factible únicamente si la empresa u organización de servicio y la empresa de sub-servicio están relacionados, o si el contrato entre ellas prevé su uso. (International Federación of accountants, 2010). Párr. 220-223.

4.3.2. Requerimientos éticos

El auditor de la empresa u organización de servicios está sujetos a los requerimientos de independencia relativos, que normalmente incluyen las partes A y B, del código de la IFAC, o los requerimientos locales, lo que sean más estrictos. Incumplimiento de un trabajo de conformidad con esta norma, el código de la IFAC, no exige que el auditor de la empresa u organización de servicios sea independiente de las entidades usuarias. (International Federación of accountants, 2010). Párr. 224.

4.3.3. La administración y los encargados del gobierno corporativo

La administración y estructura del gobierno corporativo varía según la jurisdicción y la entidad, lo que refleja influencia tales como contextos culturales y jurídicos, en el tamaño y características de la propiedad, esta diversidad significa que no es posible que esta norma especifique todos los trabajos de la (s) persona(S) con quienes interactúa el auditor de la empresa u organización de servicio, puede ser segmento de una tercera organización y no una entidad jurídica independiente. En tales casos, la identificación del personal adecuado de la administración o encargados del gobierno corporativo a los cuales se debe solicitar las declaraciones escritas, puede requerir de juicio profesional. (International Federación of accountants, 2010). Párr. 225.

4.3.2. Objetivos

Los objetivos del auditor de la empresa u organización de servicios son:

- Obtener seguridad razonable de que en todos los aspectos importantes sobre la base de criterios adecuados.

La descripción del sistema de la empresa u organización de servicios se presenta razonablemente como se diseñó y aplicó en todo el período sujeto a revisión.

Los controles relacionados con los objetivos de control establecidos en la descripción del sistema preparado por la empresa u organización de servicios fueron diseñados adecuadamente durante el período especificado. (o en el caso de tipo 1, a una fecha determinada.)

En caso de que se incluya en el alcance del trabajo, los controles operan efectivamente para proporcionar una seguridad razonable de que los objetivos de control establecidos en la descripción del sistema preparado por la empresa u organización de servicios, se cumplieron durante el período de tiempo especificado.

- Informar sobre los asuntos descritos anteriormente, de conformidad con los hallazgos del auditor de la empresa u organización de servicios. (International Federación of accountants, 2010). Párr. 240-241.

4.3.3. Requerimientos

(International Federación of accountants, 2010)El auditor de la empresa u organización de servicios no representa el cumplimiento de esta norma a menos que haya cubierto los requerimientos de esta norma y de la ISAE 3000. Párr. 270.

4.3.3.1. Requerimientos éticos

(International Federación of accountants, 2010). El auditor de la empresa u organización de servicios debe cumplir con los requerimientos éticos relevantes, que incluyen los relativos a independencia aplicables a los trabajos de aseguramiento. Párr. 271.

4.3.3.2. Administración y encargados del gobierno corporativo.

Cuando esta ISAE obligue al auditor de la empresa u organización de servicios a interrogar a, solicitar declaraciones de comunicarse con su forma de interactuar con la empresa u

organización de servicios, debe determinar las personas de la administración o estructura del gobierno corporativo de la empresa u organización de servicios con quienes interactuará. Esto incluye la consideración de las personas con responsabilidades y conocimientos relevantes sobre los asuntos en cuestión. (International Federación of accountants, 2010). Párr. 272.

4.3.4. Aceptación y continuidad.

(International Federación of accountants, 2010). Es el procedimiento de evaluación que describe la fase de la aceptación de nuevos clientes y la renovación de clientes existentes. Párr. 273.

La capacidad de competencia relevante para realizar trabajo incluye cuestiones como las siguientes:

- Conocimiento de la industria en cuestión.
- Una comprensión de la tecnología y los sistemas de información
- Experiencia entre las evaluaciones de los riesgos relacionados con el diseño adecuado de los controles.
- experiencia en el diseño y el desempeño de las pruebas y los controles y la evaluación de los resultados. (International Federación of accountants, 2010). Párr. 275.

4.3.4.1. Aceptación de un cambio en los términos del trabajo.

Una solicitud para cambiar el alcance del trabajo no puede tener una justificación razonable cuando, por ejemplo, se pide excluir cierto objetivo de control del alcance del trabajo,

debido a la probabilidad de que el auditor de la empresa u organización de servicio emita una opinión son salvedad o que la empresa u organización de servicio no proporcione al auditor de la empresa u organización de servicio una declaración escrita y se haga la petición para llevar a cabo el trabajo de acuerdo a las ISAE 3000.

Una solicitud para cambiar el alcance del trabajo puede tener una justificación razonable cuando, por ejemplo, se pida excluir del trabajo a una empresa de sub-servicio, cuando la empresa u organización de servicio no pueda arreglar el acceso del auditor del servicio, y el método utilizado para tratar con los servicios prestados por dicha empresa de sub-servicio se cambia al método de inclusión al método de exclusión. (International Federación of accountants, 2010). Párr. 277-278.

4.3.5. Evaluación de lo apropiado de los criterios.

Los criterios deben estar a disposición de los usuarios previstos para que puedan comprender las bases para soportar la aseveración de la empresa u organización de servicio sobre la presentación razonable de la descripción de su sistema, lo apropiado del diseño de los controles y en el caso de un informe de tipo 2, la efectividad operativa de los controles con los objetivos de control.

La ISAE 3000 obliga al auditor de la empresa u organización de servicios, entre otras cosas, a evaluar la idoneidad de los criterios, lo apropiado del objetivo del asunto, el objetivo del asunto es la condición subyacente de interés para los usuarios previstos del informe de aseguramiento. La siguiente figura identifica el objeto del asunto y los criterios mínimos para

cada una de las opiniones en los informes tipo 1 y tipo 2. (International Federación of accountants, 2010). Párr. 290-291.

	Objeto del asunto	Criterios	Comentario
Opinión sobre la presentación razonable de la descripción del sistema de la empresa u organización de servicios tipo 1 y 2	El sistema de la empresa u organización de servicios que probablemente sea relevante para el control de las entidades usuarias en relación con la información financiera y que está cubierta por el informe de aseguramiento de la empresa u organización de servicios	La descripción está presentada razonablemente si: 1. Señala como se diseñó e implementó el sistema de la empresa u organización de servicios incluyendo, según proceda, los asuntos identificados en el párrafo. 2. para un informe de tipo 2, incluye los detalles relativos a los cambios al sistema de la empresa u organización de servicios durante el período cubierto por la descripción, y 3. No omite ni distorsiona la	Puede ser necesario adaptar la relación específica de los criterios de esta opinión para ser coherente con los criterios establecidos, por ejemplo, con la legislación o regulación, los grupos usuarios o un organismo profesional. En la aseveración ilustrativa de la empresa organización de servicios de apéndice 1 se proporcionan ejemplos de criterios para esta opinión. Los párrafos anteriores ofrecen más orientación para determinar si se cumplen estos criterios. En cuanto a los requerimientos de la

Br. Héctor Salgado Palacios
Br. Michael Tejeda Valenzuela

		información relevante del sistema de la empresa u organización de servicios que está describiendo y reconoce al mismo tiempo que la descripción está separada para satisfacer las necesidades de una amplia gama de entidades usuarias.	ISAE 3000, la información de la materia para esta opinión es la descripción de la empresa u organización de servicios de sus sistemas y la aseveración de dicha organización de que la descripción está presentada razonablemente

Tabla 3.1: Objeto del asunto y los criterios mínimos para cada una de las opiniones en los informes tipo 1 y tipo 2

Fuente: (International Federación of accountants, 2010)

4.3.6. Materialidad

En un trabajo para informar sobre los controles en una organización de servicio, el concepto de materialidad se refiere al sistema objeto del informe, no a los estados financieros de las entidades usuarias. El auditor de la empresa u organización de servicio planifica y realiza los procedimientos para determinar si la descripción de sistemas u organización de servicio presenta razonablemente, en todos los aspectos importantes, controles de dicha organización operan eficazmente en todos los aspectos importantes.

El concepto de materialidad tiene en cuenta que el informe de aseguramiento del auditor de la empresa u organización de servicio proporciona información sobre el sistema de la empresa u organización de servicio para satisfacer las necesidades comunes de información de una amplia gama de entidades usuarias y sus auditores que entienden la manera como se ha utilizado el sistema.

La materialidad con respecto a la presentación razonable de la descripción de sistema de la organización de servicio y con respecto al sistema de los controles, implica considerar principalmente los factores cualitativos, por ejemplo: si la descripción incluye aspectos importantes del procesamiento de la transacciones significativas; si el omite o distorsiona la información pertinente; y la capacidad de los controles, según su diseño, para proporcionar una seguridad razonable de que se logró los objetivos de control.

La materialidad con respecto a la opinión del auditor de la empresa u organización de servicio sobre la efectividad operativa de los controles incluye la consideración de los factores cuantitativitos y cualitativos, por ejemplo, la tasa tolerable y la tasa observada de desviación observada (una cuestión cualitativa). (International Federación of accountants, 2010). Párr. 310-214.

4.3.7. Obtención del entendimiento del sistema de la organización del servicio.

En estos momentos, una vez realizado el mayor esfuerzo inicial que supone crear nuevos mecanismos e integrarlos en la dinámica de trabajo de los Centros, Servicios y Unidades, se ha pasado a la fase de mantenimiento y mejora de todo este entramado, que en ningún caso, supone una carga de trabajo, ni en volumen ni en intensidad, como ha supuesto hasta la fecha

Obtener un entendimiento del sistema de la organización de servicio, incluido los controles, el cual se incluye en el alcance del trabajo, ayuda al auditor de la empresa u organización de servicio a:

- Identificar los límites de ese sistema, y cómo interactúan con los otros sistemas.
- Evaluar la descripción de la empresa u organización de servicios presenta razonablemente el sistema que ha sido diseñado e implementado.
- Determinar que controles son necesarios para alcanzar los objetivos de control establecidos en la descripción del sistema de la organización de servicios.
- Evaluar si los controles fueron diseñados apropiadamente.
- Evaluar, en el caso de un informe del tipo 2, si los controles operaban eficazmente.

Los procedimientos del auditor de la empresa u organización de servicios para obtener esta comprensión pueden incluir:

- Investigar con la empresa u organización de servicios quién, a juicio del auditor de servicio puede tener la información relevante.
- Observar las operaciones e inspeccionar los documentos, informes, registros impresos y electrónicos del procesamiento de las transacciones.

- Inspeccionar una selección de acuerdo con la empresa u organización de servicios y las entidades usuarias para identificar los términos comunes.
- Reprocesar los procedimientos de control.

Obtención de la evidencia relacionada con la descripción:

Considerando que las siguientes preguntas pueden ayudar al auditor de la empresa u organización de servicios a determinar si los aspectos de la descripción incluida en el alcance del trabajo están presentados razonablemente respecto de todo lo importante:

- ¿La descripción aborda los principales aspectos del servicio proporcionado (el alcance del trabajo) que razonablemente se puede separar que sea relevante para las necesidades comunes de una amplia gama de auditores usuarias en la planificación de sus auditorías para los estados financieros de las entidades usuarias?
- ¿La descripción está preparada en tal nivel de detalle que se pueden esperar razonablemente que proporcione la información suficiente a una amplia gama de auditores usuarias para que obtenga un entendimiento de control interno de conformidad con la NIA 315?

La descripción no necesita abordar todos los aspectos de procesamiento de la empresa u organización de servicio o los servicios prestados a las entidades usuarias, ni necesita ser tan detallada que pudiera permitir a un lector comprometer los controles de seguridad o de otro tipo en la organización de servicio.

- Cuando algunos de los objetivos de control establecidos en la descripción del sistema de la empresa u organización de servicio han sido excluidos del alcance del trabajo, ¿la descripción identifica claramente los objetivos excluidos?

- ¿se ha puesto en práctica los controles indicados en la descripción?
- ¿Están descritos de manera adecuada los controles complementarios de la entidad usuarias, si los hay? En la mayoría de los casos la descripción de los objetivos de control está redactada de tal manera que es posible lograr los objetivos de control mediante la operación eficaz de los controles implementados por las empresas u organización de servicios sola. En algunos casos sin embargo los objetivos de control establecidos en la descripción del sistema de la empresa u organización de servicio no pueden ser alcanzados por la empresa u organización de servicio sola, porque su logro requiere la implementación de los controles específicos por entidades usuarias. Este puede ser el caso, por ejemplo, cuando los objetivos de controles están especificados por una autoridad reguladora. Cuando la descripción incluye los controles complementarios de la entidad usuaria, la descripción identifica por separado a dichos controles junto con los objetivos de control específico que no pueden ser alcanzados por la empresa u organización de servicio sola.

Si se ha utilizado el método inclusivo, ¿La descripción identifica por separado los controles en la empresa u organización de servicios y los controles en la empresa de sub-servicios? Si se ha utilizado el método de exclusión, ¿La descripción identifica las funciones que lleva a cabo la empresa de sub-servicios? Cuando se usa el método de exclusión, la descripción no necesita describir el procedimiento detallado ni los controles en la empresa de sub-servicios.

Los procedimientos del auditor de la empresa u organización de servicios para evaluar la presentación razonable de la descripción pueden incluir.

- considerar la naturaleza de las entidades usuarias y la probabilidad de que los servicios prestados por la empresa u organización de servicios las afecten, por ejemplo, si las entidades usuarias son de una industria en particular y si están reguladas por agencias gubernamentales.
- Leer, con las entidades usuarias, los contratos estándar o cláusulas estándar de los contratos (si procede) para entender las obligaciones contractuales de la organización de servicio.
- Observar los procedimientos realizados por el personal de la organización de servicio.
- Revisar la política y manuales de procedimientos de la empresa u organización de servicios y otros documentos de sistemas, por ejemplo, diagramas de flujo y narrativas. (International Federación of accountants, 2010). Párr. 230-241.

4.3.8. Obtención de evidencia relacionada con diseño de controles.

Desde el punto de vista de una entidad usuarios o un auditor usuarias, un control está adecuadamente diseñado si, de manera individual o en combinación con otros controles, proporciona, al cumplimiento satisfactorio, seguridad razonable de que se evita, o detecta y corrige, declaraciones erróneas de materialidad. Una empresa u organización de servicios o un auditor de servicio, sin embargo, no tienen conocimiento de las circunstancias en las entidades usuarias individuales que determinarían su una declaración errónea que resulta de una desviación de control es o no de materialidad para esas entidades usuarias.

Por otro lado, desde el punto de vista de un auditor de servicio, un control está adecuadamente diseñado, si de manera individual o en combinación con otros controles,

proporciona, al cumplimiento satisfactorio, seguridad razonable de que alcanza los objetivos de control establecidos en la descripción del sistema de la organización de servicio.

Los controles pueden consistir en una serie de actividades dirigidas al logro de un objetivo de control. En consecuencia, si el auditor de la empresa u organización de servicios considera que algunas actividades no son eficaces para lograr un objetivo de control particular, la existencia de otras actividades podría permitirle concluir que los controles relacionados con el objetivo están diseñados adecuadamente. (International Federación of accountants, 2010). Párr. 250-251.

4.3.9. Obtención de evidencia relacionada con la efectividad operativa de los controles.

Desde el punto de vista de una entidad usuarias o un auditor usuarias, un control opera eficazmente si, de manera individual o en combinación con otros controles, proporciona seguridad razonable de que las declaraciones erróneas de materialidad, ya sea por fraude o error, son prevenidas, detectadas y corregidas. Una empresa u organización de servicios o un auditor de servicios, sin embargo, no tienen conocimiento de las circunstancias en las entidades usuarias individuales que determinan su ha ocurrido una declaración errónea que resulta de una deviación de control, y de ser así, si es de materialidad.

Por lo tanto, desde el punto de vista de un auditor de servicio, un control opera eficazmente si, de manera individual o en combinación con otros controles proporciona seguridad razonable de que se logra los objetivos de control establecidos en la descripción del sistema de la organización de servicio. Del mismo modo, una empresa u organización de servicios o un auditor de la empresa u organización de servicio no están en condiciones de

determinar si alguna desviación de control observada daría lugar a una declaración errónea de materialidad desde el punto de vista de entidad usuarias individual.

Obtener el suficiente entendimiento de los controles para opinar sobre lo adecuado de su diseño no es prueba suficiente de su efectividad operativa, a menos que haya algún grado de automatización que prevea el funcionamiento consistente de los controles tal como fueron diseñándose e implementados.

Por ejemplo, obtener información sobre la implementación de un control manual en un momento, no aporta evidencia sobre el funcionamiento del control en otros momentos. Sin embargo, debido a la consistencia inherente del procesamiento de tecnología de la información (TI) realiza procedimientos para determinar el diseño de un control automatizado, y para saber si se ha dicho implementado dicho control, dependiendo de la evaluación del auditor de la empresa u organización de servicios y de las pruebas de otros controles, como las de los cambios en el programa.

Ciertos procedimientos de control quizá no dejen una constancia de su funcionamiento que pueda ser probada en una fecha posterior y, en consecuencia, el auditor de la empresa u organización de servicios puede verse en la necesidad de probar la efectividad operativa de esos procedimientos de control en varias ocasiones durante el período del informe.

El auditor de la empresa u organización de servicios ofrece una opinión sobre la efectividad operativa de los controles a lo largo de cada período, por lo tanto, se requiere suficiente evidencia apropiada sobre la operación de los controles durante el período actual para que pueda expresar dicha opinión. Sin embargo, el conocimiento de desviaciones observadas en trabajos anteriores podría ocasionar que el auditor de la empresa u organización de servicios

incrementara el alcance de las pruebas durante el período en curso. (International Federación of accountants, 2010). Párr. 260-265.

4.3.9.1. Muestreo

Cuando el auditor de la empresa u organización de servicios utilice el muestreo debe:

- Considerar la finalidad del procedimiento y las características de la población de que se tomará la muestra, al diseñar la muestra.
- Determinar un tamaño de muestra suficiente para reducir el riesgo de muestreo a un nivel apropiado bajo.
- Seleccionar las partidas de la muestra de tal forma que cada unidad de muestreo tenga probabilidad de selección.
- Si algún procedimiento diseñado no es aplicable para una partida seleccionada, aplicar el procedimiento de una partida de reemplazo.
- Si no se puede aplicar los procedimientos diseñados u otros procedimientos alternativos adecuados, en una partida seleccionada, considerar que esa partida como una desviación. (International Federación of accountants, 2010). Párr. 270

4.3.9.2. Naturaleza y causa de las desviaciones.

El auditor de la empresa u organización de servicios debe investigar la naturaleza y causa de cualquier desviación identificada y debe determinar si:

- las desviaciones identificadas están dentro de la tasa esperada de desviación y son aceptables; por lo tanto, las pruebas que fueron realizadas constituyen una

base apropiada para concluir que el control opera de manera eficaz durante todo el periodo determinado.

- Las pruebas de control adicionales u otros controles son necesarias para llegar a una conclusión sobre si los controles relativos con un objetivo particular de control, están operando con efectividad durante el período determinado.
- Las pruebas efectuadas constituyen una base apropiada para concluir que el control no funcionó con efectividad durante el período determinado. (International Federación of accountants, 2010). Párr. 278-279.

4.3.10. Trabajo de una función de auditoría interna

Le ayuda a una empresa a lograr sus objetivos mediante proporcionar un enfoque sistemático, disciplinado, para evaluar y mejorar la efectividad de la administración del riesgo, la función actuarial, la función de cumplimiento y los procesos internos de gobierno. (International Federación of accountants, 2010). Párr. 290

4.3.10.1. Obtención de un entendimiento de la función de auditoria interna

Si la empresa u organización de servicios cuenta con una función de auditoría interna, el auditor de la empresa u organización de servicios debe entender la naturaleza de las responsabilidades de esta función u de las actividades que realiza, a fin de determinar si puede ser relevante para el trabajo. (International Federación of accountants, 2010). Párr. 292

4.3.10.2. Determinar si y en qué medida se utilizará el trabajo de los auditores internos.

El auditor de la empresa u organización de servicios debe determinar:

Si es probable que el trabajo los auditores internos es adecuado para los fines de la revisión y de ser así el plan del efecto en el trabajo de los auditores internos en la naturaleza, duración o alcance de los procedimientos del auditor de la empresa u organización.

Al determinar si es probable que el trabajo de los auditores internos es adecuado para los fines de la revisión, el auditor de la empresa u organización de servicios debe evaluar:

- La objetividad de la función de auditoria interna.
- La competencia técnica de los auditores internos
- La posibilidad que el trabajo de los auditores internos se lleve a cabo con diligencia profesional.
- La disponibilidad que exista comunicación eficaz entre los auditores internos y el auditor de la empresa u organización de servicios.

Al determinar el plan del efecto del trabajo de los auditores internos sobre la naturaleza, duración o alcance de los procedimientos del auditor de la empresa u organización de servicios, debe considerar:

- La naturaleza y el alcance del trabajo específico realizado, o que será realizado, por los auditores internos.
- La importancia de dicho trabajo para las conclusiones del auditor de la empresa de servicios.

- El grado de subjetividad involucrado en la evaluación de la evidencia obtenida para soportar dichas conclusiones. (International Federación of accountants, 2010). Párr. 295.

4.3.10.3. Utilización del trabajo de la función de auditoria interna.

Con objeto de que el auditor de la empresa u organización de servicios pueda utilizar el trabajo específico de los auditores internos, debe evaluar y realizar procedimientos a dicho trabajo para determinar si es adecuado para sus fines.

Para determinar si el trabajo específico realizado por los auditores internos adecuado para los fines del auditor de servís, debe evaluar si:

- El trabajo fue realizado por auditores internos quienes cuentan con formación técnica y competencias adecuadas.
- El trabajo fue supervisado, revisado y documentado adecuadamente.
- Se ha obtenido evidencia adecuada para permitir a los auditores internos formar conclusiones razonables.
- Las conclusiones a las que se llegó son apropiadas en las circunstancias y los informes preparados por los auditores internos son consistentes con los resultados del trabajo realizado.
- Las excepciones de interés para el trabajo o los asuntos inusuales revelados por los auditores internos son resueltas, apropiadamente. (International Federación of accountants, 2010). Párr. 297-299.

4.3.11. Declaraciones escritas.

El auditor de la empresa u organización de servicios debe solicitar a la empresa u organización de servicios que agregue declaraciones escritas de lo siguiente:

- Que confirme las aseveraciones relativa a la descripción del sistema.
- Que ha proporcionado al auditor de la empresa u organización de servicios, toda la información relevante y el acceso acordado.
- Que ha revelado al auditor de la empresa u organización de servicios cualquiera de los siguientes asuntos sobre los que tenga conocimiento Del incumplimiento de leyes o regulaciones, fraudes o desviaciones sin corregir imputables a la organización de servicios, que pueden afectar a una o más entidades usuarias, deficiencias en el diseño en los controles; casis en que los controles no han funcionado como se describe y cualquier hecho posterior al período cubierto por la descripción del sistema de la organización de servicios y hasta la fecha del informe de aseguramiento del auditor de la empresa y organización de servicios, que pudiera tener un efecto significativo sobre dicho informe. (International Federación of accountants, 2010). Párr. 302-305.

4.3.12. Otra información

El auditor de la empresa u organización de servicios debe leer otra información, si la hubiese, incluida en un documento conteniendo la descripción del sistema de la organización de servicios y el informe de aseguramiento del auditor de la empresa de servicios. Para identificar las inconsistencias materiales, si las hubiese, con esa descripción. Al realizar esto, el auditor de

la empresa u organización de servicios de servicios podría percatarse de algún aparente error material en esa otra información.

Si el auditor de la empresa u organización de servicios se percata de alguna inconsistencia material o alguna declaración errónea en la otra información, debe discutir este asunto con la organización de servicios. Si concluye que hay alguna inconsistencia material o alguna declaración errónea en la otra información que la organización de servicios se niega a corregir, debe adoptar las medidas correspondientes. (International Federación of accountants, 2010). Párr. 306-307.

4.3.13. Hechos posteriores

El auditor de la empresa u organización de servicios debe investigar si dicha organización tiene conocimiento de cualquier hecho posterior al periodo cubierto por la descripción de su sistema y hasta la fecha del informe de aseguramiento del auditor, que pudiera tener algún efecto significativo sobre dicho informe. Si tiene conocimiento de algún hecho y dicha información no es revelada por la organización de servicios, debe revelarla en su informe de aseguramiento.

El auditor de la empresa u organización de servicios no está obligado a realizar algún procedimiento relacionado con la descripción del sistema de la empresa u organización de servicios, sobre lo adecuado del diseño o efectividad de los controles, después de la emisión de su informe de aseguramiento. (International Federación of accountants, 2010). Párr. 309-310.

4.3.14. Documentación

El auditor de la empresa u organización de servicios debe preparar la documentación necesaria que permita a algún auditor experimentado, que no tenga relación previa con el trabajo, entender:

- La naturaleza, oportunidad y alcance de los procedimientos realizados para cumplir con esta ISAE y los requerimientos legales y regulatorios relativos.
- El resultado de los procedimientos realizados, y de la evidencia obtenida.
- Y los asuntos significativos que surgieron durante el trabajo, y las conclusiones alcanzadas al respecto, así como los juicios profesionales significativos realizados para llegar a esas conclusiones.

Al documentar la naturaleza, la oportunidad y alcance de los procedimientos realizados, el auditor de la empresa u organización de servicios debe documentar:

- Las características que identifican a las partidas o asuntos específicos que están siendo probados.
- Quien realizó el trabajo y la fecha en que se completó dicho trabajo.
- Quien revisó el trabajo realizado, la fecha y alcance de la revisión.

Si el auditor de la empresa u organización de servicios encuentra que es necesario modificar la documentación de trabajo existente o añadir nuevos documentos después de que se ha completado el archivo final del trabajo y que dicha documentación no afecta su informe, debe, independientemente de la naturaleza de las modificaciones o adicciones, documentar:

- Las razones específicas para llevaras a cabo y cuándo y por quien fueron hechas y revisadas. (International Federación of accountants, 2010). Párr. 315-318.

4.3.15. Preparación del informe de aseguramiento del auditor de la empresa u organización de servicio.

El informe de aseguramiento del auditor de la empresa u organización de servicios debe incluir los siguientes elementos básicos:

- Título que indique claramente que es un informe de aseguramiento del auditor de la empresa u organización de servicios independientes.
- Destinatario
- Identificación de la descripción del sistema de la empresa u organización de servicios y la aseveración que incluye los asuntos antes descritos.
- Identificación de aquellas partes del sistema de la empresa u organización de servicios, si las hubiera, que no son cubiertas por la opinión del auditor de la empresa u organización de servicios.
- Identificación de los criterios y la parte de los objetivos de control.
- Una declaración de que el informe y en el casi de un informe tipo 2, las descripciones de las pruebas de los controles están destinados únicamente para las entidades usuarias y sus auditores, que tienen un conocimiento suficiente para considerarlo, junto con otros datos que incluyen la información sobre los controles operados por las propias entidades usuarias, al evaluar los riesgos de errores materiales de los estados financieros de las entidades usuarias.
- Una declaración de que el trabajo fue realizado de conformidad con la ISAE 2402, informe de aseguramiento sobre los controles establecidos en una empresa u organización de servicio.

- Un resumen de los procedimientos que el auditor de la empresa u organización de servicios llevó a cabo para obtener una seguridad razonable y una declaración de que la evidencia obtenida es suficiente y apropiada para proporcionar una base razonable para sustentar su opinión. (International Federación of accountants, 2010). Párr. 321-325.

4.3.16. Otras responsabilidades de comunicación.

Si el auditor de la empresa u organización de servicios llega a tener conocimiento de incumplimiento con alguna ley o regulación, fraude o errores no corregidos imputables a la empresa u organización de servicios, que no sean claramente triviales y puedan afectar a una o más entidades usuarias, debe determinar dicho asunto ha sido comunicado apropiadamente a las entidades usuarias afectadas. Si el asunto no ha sido objeto de dicha comunicación y la empresa u organización de servicios no está dispuesta a llevar a cabo dicha comunicación, el auditor de la empresa u organización de servicios debe tomar medidas adecuadas. (International Federación of accountants, 2010). Párr. 327.

4.3.16. Otras responsabilidades de comunicación

Las medidas adecuadas para responder a las circunstancias identificadas pueden incluir:

- Obtener asesoría legal sobre las consecuencias de los diferentes cursos en acción.
- Comunicarse con los encargados del gobierno corporativo de la organización de servicio.

- Comunicarse con terceros (por ejemplo, una entidad de regulación) cuando se requiera.
- Modifica la opinión del auditor de servicio, o añadir un párrafo de otro asunto.
- Retirarse del trabajo.

Los requerimientos éticos y que planifiquemos y realicemos nuestros procedimientos para obtener una seguridad razonable de que, en todos los aspectos materiales, la descripción está presentada razonablemente y los controles están diseñados adecuadamente y operan con efectividad. (International Federación of accountants, 2010). Párr. 335-336.

V. Caso Práctico

Caso práctico de la aplicación de una Auditoria de Tecnología de la Información a la entidad NP Enterprise Inc. en base a los marcos normativos COBIT 5.0 y la Norma NITA 3402.

5.4.1. Introducción

El proceso de auditoría aplicado a la empresa NP Enterprise Inc., se desarrolló empleando los marcos normativos COBIT 5.0 y la norma ISAE 3402, la cual provee una serie de fases como guía para la realización de todo el proceso de auditoría, para seleccionar el área a auditar, se evaluó los diferentes departamentos de la empresa, seleccionándose el área donde se manejan los procesos informáticos, A continuación, se describe el desarrollo de la auditoría a la empresa NP Enterprise Inc.

5.4.2. Preliminar

El examen que conforma una Auditoría TI abarca una serie de controles, verificaciones y juicios que concluyen en un conjunto de recomendaciones y un Plan de Acción. Es la elaboración de este Plan de Acción lo que diferencia a la Auditoría TI de lo que sería una auditoría tradicional, La Auditoria en Tecnologías de la Información y Comunicación (TIC) tienen elementos que, aunque no parezcan importantes son esenciales para determinar los diferentes tipos de vulnerabilidades y deficiencias existentes de los Sistemas de Información en la actualidad.

En el presente caso de Aplicación de Auditoria en Tecnologías de la Información y Comunicación analizaremos los sistemas de información de la Empresa NP Enterprise Inc. para

realizar una Auditoria en general a los sistemas de información que se implementaron, con el propósito de detectar errores, posibles problemas o situaciones en donde se estén produciendo fallos de seguridad, integridad de la información, medir los riesgos y evaluar los controles en el uso de las tecnologías de información, haciendo uso de técnicas y estrategias de análisis, que permitan que la auditoría informática se convierta en una real y eficiente herramienta de gestión de tecnologías de información.

5.4.3. Antecedentes de la Entidad

NP Enterprise Inc. se fundó el 08 de abril de 1997 en Managua, Nicaragua con capital privado nacional, llegándose a consolidar en poco tiempo como una de las empresas líderes en servicios integrales de seguridad física y electrónica. Hoy en día NP Enterprise Inc. es una de las principales empresas nacionales de seguridad, pionera en servicios innovadores e integrales de seguridad.

NP Enterprise Inc. es parte del Grupo Intertechsec S.A, la corporación centroamericana más grande de la región que aglutina a más de 12,000 colaboradores desde Guatemala hasta Panamá.

NP Enterprise Inc. tiene sus oficinas principales en Managua y oficinas departamentales en Rivas, Chinandega, Estelí, Boaco, Nandaime y Bluefields. Asimismo, es la única empresa con cobertura comprobada en todo el territorio nacional y con capacidad de brindar servicios nacionales e internacionales bajo un mismo grupo.

5.4.4. Perfil Integral Institucional

La empresa NP Enterprise Inc. es una empresa especialista en donde se ofrece una amplia gama de productos y servicios de seguridad física, electrónica, consultorías y capacitaciones; cimentamos nuestra eficacia en más de 24 años de experiencia, lo que además nos permite, brindar soluciones integrales de seguridad adaptadas a las necesidades y capacidad financiera de los clientes.

5.4.4.1. Misión

Somos una empresa de servicio de seguridad dedicada a proveer tranquilidad a sus clientes en la región por medios de soluciones integrales de seguridad. Combinamos la mejor Tecnología, Recursos Humanos certificados y procesos comprobados para garantizar la calidad de nuestros Servicios.

5.4.4.2. Visión

Convertirnos en la empresa de Seguridad que ofrece el Servicio de mejor Calidad, en Recursos Humanos y Tecnología en la región, produciendo beneficios permanentes a los Accionistas, Clientes, Colaboradores y a la Comunidad.

5.4.4.3. Valores

- Honestidad

Hablar y obrar con sinceridad, actuar con decencia y honradez, administrar adecuadamente lo que se tiene a cargo.

- Orden

Conjunto de normas necesarias para lograr un objetivo deseado, para la organización de las cosas, la distribución del tiempo y la realización de la actividad humana.

- Respeto:

Tratar a las otras personas como a ti mismo, apreciar y valorar a las personas como a mí mismo, todo ser humano merece un trato digno.

- Responsabilidad:

Cumplir con el deber de asumir las consecuencias de mis actos, rendir cuentas ante nosotros mismos, ante la familia, ante mis jefes y compañeros, ante mis clientes, ante la sociedad y ante Dios.

5.4.4.4. Estructura organizacional.

La empresa NP Enterprise Inc. es una empresa de productos y servicios de seguridad física, electrónica, los servicios que estos ofrecen son:

- Seguridad física
- Seguridad electrónica
- Carretera segura (Vigilancia)
- Poligrafía
- Verificaciones y cobertura satelital (GPS)

La empresa cuenta con dos áreas principales que son el departamento de vigilancia y control y el de sistemas de seguridad y mantenimiento, siendo esta última donde se manejan las operaciones esenciales de los procesos informáticos, aquí se manipulan los dos sistemas

utilizados para la gestión de los distintos servicios que la empresa brinda, de esta área se alimentan las más áreas, a través de la red interna que les brinda conexión a Internet e intercomunicación entre los sistemas.

Esta área cuenta con treinta y seis empleados, quienes hacen uso de los equipos que se encuentran en el departamento, entre ellos se encuentra el jefe de ingeniería quien está a encargo del control de uso de equipos y software. (Ver anexo 2)

5.4.5. Planteamiento del problema

Empresas de éxito han reconocido que el comité y los ejecutivos deben aceptar las TI como cualquier otra parte importante de hacer negocios. Los comités y la dirección Empresas de éxito han reconocido que el comité y los ejecutivos deben aceptar las TI como cualquier otra parte importante de hacer negocios. Los comités y la dirección tanto en funciones de negocio como de TI deben colaborar y trabajar juntos, de modo que se incluya la TI en el enfoque del gobierno y la gestión.

La empresa NP Enterprise Inc., empresa que se dedica a la seguridad física, las actividades que se realizan en esta empresa son de diversos tipos tales como: venta de productos y servicios de seguridad física, electrónica, consultorías y capacitaciones, entre otros. Esta empresa como parte de su crecimiento hace uso del ambiente de TI para sistematizar las áreas del negocio y así ofrecer servicio de calidad a sus clientes.

Es por ello que la entidad, usando como base la auditoría, trata de evaluar de forma particular cada proceso del negocio y así identificar fortalezas y debilidades en la gestión de procesos informáticos de dicha empresa.

Con los resultados obtenidos en la auditoría pretende fortalecer aquellos procesos que presenten debilidades en la revisión y evaluación de controles, sistemas, comunicaciones y procedimientos informáticos de la empresa.

Al llevar a la práctica las recomendaciones obtenidas en la auditoría informática se espera aumentar la eficiencia y seguridad de la información y así mismo el proceso de toma de decisiones.

5.4.6. Justificación

Con la ejecución de la auditoría a la empresa NP Enterprise Inc. se evaluará la eficiencia del manejo de la información y los procesos de la empresa, lo cual requiere vigilar los procesos de recopilación, proceso y almacenamiento de la información dentro de la empresa, todo esto mediante el uso de la tecnología informática; en toda entidad este proceso es vital para el buen funcionamiento de la misma.

Tomando en cuenta la evaluación preliminar y la planificación de auditoria (Ver anexo 3), en la empresa se definió como área para la ejecución de auditoría, el área de instalaciones y mantenimientos, que es donde se manejan las operaciones referentes a los procesos informáticos de la entidad.

5.4.7. Formalización

El proceso de realización de esta auditoría se acordó de manera formal con la alta dirección de la empresa NP Enterprise Inc., en una reunión donde se convino entre el gerente general y los auditores, el área a auditar, los límites y alcances de la misma, visitas y tiempo de evaluación.

Las áreas a evaluar fueron analizadas mediante los procedimientos y evaluando el riesgo por área implementando una matriz de riesgo (Ver anexo 4,5,6 y 7) y los procedimientos del Estándar de COBIT 5.0 tomadas en distintas áreas realizando y el cual establece cuatro dominios. Debido al tiempo de ejecución, el análisis de esta auditoría se basará en los siguientes dominios: Adquisición e implementación **(**Build, Adquisition and implementation (BAI)), Entregar, dar servicios y soporte (Delivery Service and Support (DSS)), así mismo de estos dos dominios no se usarán todos los subprocesos efectuando una guía de implementación de componentes y procesos (Ver anexo 8).

5.4.8. Desarrollo

Como resultado de aplicar las técnicas y herramientas en la auditoría de TI, se evidenciaron las siguientes situaciones:

5.4.8.1. Seguridad Lógica

Al evaluar los componentes descritos en seguridad lógica, se encontraron los siguientes hallazgos los que se describen a continuación:

5.4.8.1.1. Componentes:

V.4.8.1.1.1 Acceso de los usuarios a sistemas, sistemas operativos y bases de datos.

En el apartado de acceso de los usuarios a sistemas, sistemas operativos y bases de datos, se pudo evidenciar que los usuarios tienen libre acceso al sistema operativo de las computadoras a excepción de la computadora del encargado, esta tiene contraseña para acceder

al sistema operativo Windows y las demás no, aquí se evidenció que ninguna PC tiene contraseña de arranque y basta con encenderla para cargar el sistema.

En cuanto al acceso de los usuarios a sistemas se encontró que en la empresa se emplean 4 sistemas de información, los que requieren contraseña para poder acceder. El primero es el sistema proporcionado por la Dirección General de Aduana Nicaragüense, que es el SIDUNEA WORLD, este es un sistema online, el cual requiere obligatoriamente de conexión a Internet para su uso, este sistema necesita de usuario y contraseña para el acceso, los permisos de acceso son proporcionados por la aduana a agentes aduaneros inscritos y con permiso legal otorgado por la misma aduana.

En la empresa existen dos empleados que tienen contraseña propia para el acceso a este sistema, los demás no tienen usuario ni contraseña y en caso de que estos utilizaran el sistema uno de los dos usuarios que cuentan con acceso ingresan al sistema para que ellos lo utilicen, sin darles a ellos la contraseña y el usuario, cabe destacar que como este es un sistema que no es de la empresa, solo se evaluó el resguardo de la contraseña de acceso, así como la cantidad de usuarios que lo usan y las actividades que se realizan en él, en lo cual se evidencio que este sistema es usado por las cinco personas que laboran en el área, solamente dos de estas poseen acceso al sistema; este sistema se usa para poder registrar hacia la Dirección General de Aduanas las declaraciones que se ingresan en el sistema TCO que es el que la empresa utiliza para estas gestiones; las contraseñas son manejadas exclusivamente por los agentes aduaneros en el caso del SIDUNEA, para el TCO cada usuario tiene su contraseña y solamente el jefe de operaciones tiene la contraseña y usuario de administrador en el TCO.

El segundo sistema empleado es el TCO este es un sistema de gestión de operaciones aduaneras, este sistema fue comprado a terceros, y es administrado por el encargado de la

división de operaciones. Para el acceso a este sistema se necesita usuario y contraseña, según la información obtenida cada empleado del área tiene su usuario y contraseña para acceder al sistema, es decir que son cinco los usuarios del sistema.

El tercer sistema empleado es el sistema administrado por la Dirección General de Ingresos llamado Ventanilla Electrónica Tributaria (VET), en donde la DGI entrega accesos a los usuarios que designe la entidad, no obstante, se observó que, solo se utiliza un usuario para realizar todos los tramites tributarios de la entidad de 4 usuarios entregados

El cuarto sistema empleado por la empresa es un sistema creado en la entidad por la oficina de Informática con el nombre de Sistema Integrada de Administración Financiera SIAF_NP, la oficina de informática cuenta con 4 empleados que administran el desarrollo del sistema, base de datos de la entidad y la administración de los mismo, teniendo cada uno roles de servicios para los que fueron asignados, en donde abarca cada una de sus funciones:

- Jefe de Oficina de informática: Tiene acceso a todos los servicios de la Oficina
- Programador Front- End: Tiene acceso al desarrollo de capa de presentación
- Programador Back- End: Tiene acceso al desarrollo de capa de acceso de datos y conexión a la base de datos
- Administrador de Bases de datos: Tiene acceso a desarrollo y mantenimiento de las bases de datos de la empresa

La aplicación correcta de los controles de acceso a los sistemas en una empresa es vital porque aumenta la seguridad e integridad de la información, se disminuye el riesgo de fraude y de filtración o alteración de la información, limitando enormemente la cantidad de usuarios y administradores de los puntos críticos de TI y mantener el control del flujo de la información.

5.4.8.1.1.2 Acceso de los usuarios a programas y archivos

En este aspecto se obtuvo información mediante observación y entrevistas, por lo que se pudo evidenciar que las políticas de la empresa establecen que los trabajadores que utilizan las computadoras únicamente poseen la potestad de hacer uso de los sistemas TCO, Sidunea World, VET, SIAF_NP, la paquetería de herramientas ofimáticas Office y Outlook para el uso del correo institucional. Tienen prohibido el uso de programas ajenos a la misión del negocio.

Estas prohibiciones son informadas a los empleados de forma verbal, por medio de la encargada de administración y del responsable del área de operaciones, además de mantener en lugares visible rótulos con el reglamento impreso.

Este control es sumamente importante ya que el empleador deja en claro a los empleados cuales son responsabilidades, derechos y restricciones en la empresa, este control mal empleado podría causar serios daños en los equipos, software y demás elementos relacionados con TI.

5.4.8.1.1.3. Disposición de sistemas alternos en caso de fallos.

En cuanto a la disposición de sistemas alternos en caso de fallos, se determinó que la empresa no cuenta con sistema alterno, tampoco tienen plan de respaldo en caso de fallas en el sistema principal. Cuando existen fallos en alguno de los sistemas de gestión aduanera recurren al proveedor de Internet o al técnico de mantenimiento, pero esto se hace solo si existe un fallo.

La utilización de sistemas alternos es vital para la prevención de caídas de servicio por largos períodos de tiempo, si una empresa no tiene sistemas alternos para funcionar en caso de que el sistema principal presente algún inconveniente, la empresa podría detener parcial o

totalmente sus operaciones, lo que se traduce en pérdidas, las que pueden ser cuantiosas para la empresa.

5.4.8.1.1.4. Existencia de software de protección (antivirus, firewall.)

Al revisar la existencia de software de protección se encontró que el antivirus utilizado en todos los equipos de la empresa es el ESET Nod 32 Versión 8.2.2 con licencia por un año, la licencia fue proporcionada por la empresa subcontratada para el mantenimiento de las computadoras en la empresa, también el firewall en uso es el firewall nativo del sistema operativo Windows 10 y en el caso de la computadora que actúa como servidor Windows 10 en donde se evidencia que las licencias de los sistemas operativos que tiene la entidad no están activadas y utilización de software orientados a cada tarea específica ya que un sistema operativo de uso comercial no puede ser utilizado como entorno de servidor nativo de la empresa

La existencia de software de protección actualizada es indispensable para la integridad y manejo de la información de la empresa, informáticamente hablando es importante contar con software que sea capaz de proteger la información digital de la empresa, este software se encarga de que la información no sea sustraída por terceros o dañada por algún software malicioso.

5.4.8.1.1.5. Control de Acceso de los usuarios a los servicios de Internet.

Cuando se revisó el control de acceso de los usuarios a los servicios de Internet se evidenció que solo las computadoras de los encargados de áreas tienen acceso a Internet, las demás computadoras solo están conectadas a la red de la empresa, pueden verse entre ellas, pero no tienen acceso a Internet.

El acceso a Internet se restringe mediante la configuración de cada PC, en el centro de redes de Windows se cambia las configuraciones para decidir qué dirección IP tiene acceso y cual no, esto lo aplica la empresa de soporte Dátate, mediante indicaciones de la alta gerencia de la empresa, quien decide los permisos de acceso a Internet, para lo cual se toma en cuenta el cargo y función de los empleados, siendo así los jefes de departamentos los únicos con acceso a Internet, el resto de equipo solo tiene acceso a la red local.

Mantener el control de los permisos de acceso a internet, disminuye los riesgos que puedan afectar la integridad de la información, además que garantiza que la comunicación a través de dicho enlace sea utilizada para los fines y objetivos de la empresa.

5.4.8.2. Seguridad Física

Al evaluar los componentes descritos en seguridad física, se encontraron los siguientes hallazgos, los que se describen a continuación:

5.4.8.2.1. Componentes:

5.4.8.2.1.1. Control de accesos de los usuarios a los equipos.

En el control de accesos de los usuarios a los equipos informáticos, se evidenció que solo los usuarios que trabajan en el área de operaciones tienen acceso a los equipos, exceptuando al personal que hace mantenimiento a los equipos, que es personal externo a la empresa.

El uso de controles para el acceso a equipos evita la exposición tanto de la información como de los equipos a riesgos provocados por accidentes o acciones mal intencionadas. Dando mayores garantías de la disponibilidad e integridad de la información.

5.4.8.2.1.2. Informes de accesos y visitas a las instalaciones.

En los informes de accesos y visitas a las instalaciones, se encontró que la empresa no lleva registro de control de ingreso al edificio, las notificaciones para el ingreso se hacen de manera verbal y no hay ningún soporte.

Además al ingresar a la empresa no se solicita ninguna identificación únicamente preguntan hacia donde se dirige y a quien busca, en el caso de las personas que llegan a la empresa a realizar mantenimiento a las PC llegan debidamente identificados a la empresa y aunque no existe un plan de mantenimiento, la encargada del área de administración lleva un control de lo que los técnicos realizan en cada visita, así mismo se lleva un registro de cambio de equipos y piezas, así como del Hardware descartado.

Mantener un control de visitas y control de presencia de personal externo en una organización, es importante porque de esta manera se mantiene un ambiente seguro para el personal que labora en la empresa; así también se protegen los activos, la continuidad operacional y la propiedad intelectual.

5.4.8.2.1.3. Inventario de equipos y software

En el inventario de equipos y software, se evidenció que la empresa cuenta con un almacén donde se encuentran las computadoras y equipos electrónicos que ya no funcionan, tienen un inventario manual de estos equipos con un diagnóstico donde se detallan piezas dañadas y piezas en funcionamiento, entre estos están: PC, impresoras, sistemas operativos en uso, etc.

Existe una computadora utilizada por el jefe de operaciones que su plataforma es Windows 10, esta actúa como servidor para el sistema aduanero TCO, este tiene una arquitectura cliente-servidor, las demás máquinas de esta área funcionan como cliente.

Es importante tener inventario de hardware y software al día, así la empresa tiene control directo sobre sus activos de TI y sabe exactamente con lo que cuenta, lo que almacena y lo que tiene que adquirir en caso de alguna modificación en TI.

5.4.8.2.1.4. Revisión de la red (factor ambiental, físico y humano)

La red está compuesta por cableado plano en su mayoría, el ISP que en este caso es Dátate, les proporciona un nodo de conexión satelital, con una antena ubicada en la parte este de la empresa, la cual se conecta a un Reuter ubicado en el área de operaciones mediante un cable UTP categoría 5e, de aquí la red se divide en cuatro subredes que son, operaciones, administración, bodega y gerencia.

La auditoría se llevó a cabo en el edificio donde se encuentran las áreas de operaciones y administración; en el área de operaciones se encuentra el Reuter de la empresa, ubicado en una repisa, fuera del alcance de los empleados, cercano al Reuter se encuentra un tomacorriente, la conexión de la antena hacia el Reuter es por el exterior; en esta conexión no existe ningún dispositivo que logre fijar y mantener la conexión estable, esto quiere decir que el medio por el que viajan los datos (Cable UTP cat. 5e) no está asegurado por ninguno de sus lados. En la red LAN las conexiones (cables UTP cat. 5e) van en canaletas y por encima del cielo falso de la oficina hasta llegar a la cercanía de las máquinas, donde se conecta directamente al puerto de red de las PC, ninguno posee una toma de datos, se pudo observar que el único estándar para cableado estructurado que se cumple en el proceso de

transmisión de datos es EIA/TIA 569. También se observó que los equipos de comunicación no cuentan con las condiciones ambientales establecidas por los estándares.

Cabe destacar que en lo que respecta a la seguridad del área mediante cámaras de seguridad y extintores, únicamente existe un extintor por área y no hay existencia de cámaras de seguridad para la protección de sus activos, esto es una debilidad que muestran en este aspecto.

La seguridad de la red es un factor importante que cualquier administrador o instalador de red debe considerar, ya que se debe garantizar la máxima seguridad de los datos que serán transmitidos a través de ella, así como la capacidad de transmisión que la empresa requiera, así que se deber tomar en cuenta todos estos aspectos al momento de una revisión, la cual debe hacerse cada cierto período de tiempo según la empresa lo considere necesario.

5.4.8.2.1.5. Controles para la instalación y uso de dispositivos externos

En lo que se refiere a los controles para la instalación y uso de dispositivos externos, se descubrió que la empresa tiene una fuerte política de restricciones de uso en lo que concierne a sus equipos de informática, los puertos USB de las computadoras están bloqueados, no está permitido el uso de ningún dispositivo externo y si un trabajador tratara de utilizarlos, este sería sancionado por la empresa.

Los controles para instalación de hardware y software evitan que empleados descontentos cometan fraude, llevándose información confidencial o que instale software innecesario.

5.4.8.3. Respaldos y planes de contingencia

Al evaluar los componentes descritos en respaldos y plan de contingencia, se encontraron los siguientes hallazgos los que se describen a continuación:

5.4.8.3.1. Componentes:

5.4.8.3.1.1. Respaldo de información crítica

En los respaldos de información crítica, se encontró que se maneja un respaldo de la información de los clientes únicamente en físico, y están resguardados en las instalaciones de la empresa, no hay respaldo digitalizado de la información, la empresa no posee redundancia en este apartado.

El respaldo de la información crítica es lo más importante de TI en una empresa, se necesita salvaguardar la información que la empresa posea, las empresas deben ser cautelosas con su información, para asegurar que sus operaciones no sean afectadas por accidentes o desastres. La existencia de respaldos actualizados puede ser la solución para una pronta recuperación de sus actividades comerciales.

5.4.8.3.1.2. Plan de Continuidad

En cuanto al plan de continuidad, la empresa no está preparada en caso de que algún desastre natural llegara a interrumpir sus acciones, la empresa no tiene contemplado que algo así pudiera interrumpir sus operaciones. Si hay algún fallo general, la empresa quedaría deshabilitada, no existe un plan de continuidad.

El plan de continuidad es necesario que sea funcional en una entidad ya que, si ocurriera algún contratiempo de fuerza mayor como un desastre natural, la empresa no quedaría fuera de operaciones, por lo tanto, no tendría pérdidas.

5.4.8.3.1.3. Plan de Contingencia

En casos de fallos de los sistemas de información el proceso que se lleva a cabo en la empresa es: Si falla el acceso al SIDUNEA WORLD a causa de la pérdida de conectividad a Internet, la empresa tiene convenios con algunas empresas aduaneras a nivel nacional para poder continuar las operaciones de la empresa, en el caso de que el TCO llegara a fallar, las gestiones que se realizan en este sistema se realizarían manualmente.

El plan de contingencia es importante ya que si ocurriera algún fallo que pueda interrumpir parcialmente las actividades de la empresa, la misma no quedaría fuera de operaciones, por lo tanto, no tendría perdidas.

5.4.8.3.1.4. Plan de Mantenimiento de Hardware y Software

En el plan de mantenimiento se encontró que la empresa tiene un contrato de soporte que puede variar según la estación del año, en verano se realiza cada 3 meses y en invierno cada 6 meses, lo que indica que el mantenimiento se realiza 3 veces en el año, este mantenimiento se podría considerar como un mantenimiento preventivo; el mantenimiento correctivo solo se hace cuando alguna computadora presenta problemas; cabe destacar que este mantenimiento lo hace una empresa subcontratada como servicios profesionales, el mantenimiento del software solo es correctivo, solo se hace cuando el software funciona mal, este mantenimiento es realizado por personal externo que está contratado por la empresa para realizar mantenimiento del software de

facturación y el de contabilidad. La empresa está clara que el mantenimiento preventivo es esencial para el buen funcionamiento de los equipos informáticos.

Es importante conocer lo que los técnicos encargados de los mantenimientos les hacen a las PC, para esto se necesita tener un plan de mantenimiento, así si se realiza algún cambio de técnico en la empresa, tanto el técnico nuevo como los directivos de la empresa estarán al tanto de lo que hacía el técnico anterior y no se tendrán futuros inconvenientes.

5.4.8.4. Documentación de Hardware y Software

Al evaluar los componentes descritos en la documentación de Hardware y Software, se encontraron los siguientes hallazgos los que se describen a continuación:

5.4.8.4.1. Componentes:

54.8.4.1.1. Disposición de manuales de usuario y de instalación de los sistemas

En la disposición de manuales de usuario y de instalación de los sistemas, se encontró que en los dos sistemas que actualmente están en uso, que son SIDUNEA WORLD y TCO, existe documentación. En el caso del SIDUNEA WORLD que es un sistema gratuito que la aduana nicaragüense proporciona, toda la documentación correspondiente a dicho sistema se encuentra en la página gubernamental de la aduana nicaragüense, en cuanto al sistema TCO de gestiones aduaneras, la empresa mantiene documentación en cuanto al manual de usuario, pero no mantiene ni los instaladores, ni el manual de instalación, esto se debe a que la adquisición del software no ha sido concretada y por el momento el proveedor de dicho software ha llegado a la empresa únicamente a instalar el software y a dejar el manual de usuario.

Es importante para el administrador del sistema como para los usuarios tener documentación de los sistemas de información, porque así es más fácil capacitar a los usuarios en el uso correcto y eficiente del software con ayuda del manual de usuario, al igual que si se requiere de instalarlo nuevamente se debe contar con un manual para que la instalación termine con éxito.

5.4.8.4.1.2. Existencia de documentos de adquisición de equipos y software y contratos legal de proveedor de Internet y red (ISP).

Al comprobar la existencia de documentos de adquisición de equipos y software y contratos legales de ISP, se encontró que la empresa cuenta con la documentación, resguardados por el área contable, en cuanto al contrato de ISP no fue mostrado solo se sabe que se contrató el ancho de banda y que el proveedor es Claro. En cuanto al proveedor de equipos informáticos se conoció que la empresa trabaja siempre con la empresa COMTECH.

La implementación de este control en la empresa es importante, porque es necesario que la empresa posea los documentos legales de adquisición de equipos, ya que si se presenta algún defecto en algún equipo nuevo se debe tener la cobertura de la garantía, así como para posibles auditorías o investigaciones, con lo cual se pueda corroborar la adquisición legal de los equipos.

5.4.8.4.1.3. Documentación de los sistemas utilizados para los servicios de la empresa

En cuanto a la documentación de los sistemas utilizados para los servicios de la empresa, se evidenció que la empresa no posee documentación, esto se debe a que los sistemas utilizados por la empresa, son sistemas enlatados, es decir sistemas comprados y desarrollados por terceros, cabe destacar que la compra del sistema TCO aún no es total,

solo se ha comprado la utilización del software, no se ha comprado los derechos de modificación del código del mismo, por lo tanto la empresa no posee la documentación, diagramas y jerarquías del software.

La falta de documentación de los sistemas en una empresa se podría traducir como un manejo ineficiente de los sistemas, por lo tanto, no se podría explotar a toda su capacidad el software.

5.4.9. Informe de Auditoria

5.4.9.1. Objetivo

Realizar valoración de los resultados obtenidos en el proceso de auditoría informática, aplicado a la empresa NP Enterprise Inc.

5.4.9.2. Alcance

La realización de esta auditoría se llevó a cabo en la empresa NP Enterprise Inc., en un período de 60 días, en el cual se abordó la evaluación del área de operaciones de la empresa, que como se explicó anteriormente es el área donde se llevan a cabo los procesos informáticos de la entidad. Se evaluó seguridad física, seguridad lógica, respaldos de datos, planes de mantenimiento, contingencia y continuidad, así como la documentación general y específica sobre equipos, sistemas y software utilizado en la empresa.

Debido al acuerdo entre la gerencia de la empresa y los auditores, no se evaluó mediante pruebas sustantivas la seguridad de la red y los sistemas de información, ya que para ellos, esto podría dar lugar a que los auditores tuvieran acceso a información valiosa y confidencial de la

empresa; por la razón antes mencionada solamente se verificó el cumplimiento de las normativas internacionales en seguridad, las que se comprobaron generalmente utilizando la información obtenida en las entrevistas, cuestionarios y mediante la observación.

5.4.9.3. Informe de aseguramiento de la empresa u organización de servicios

A: NP Enterprise Inc.

Alcance

Hemos sido contratados para informar sobre la descripción de la empresa u organización de servicios NP Enterprise Inc. de los sistema y ambiente de TI para procesar las transacciones de los clientes durante el período comprendido del 01 de enero al 31 de diciembre del 2016 y sobre el diseño y la operación de los controles relacionados con los objetivos de control establecidos en dicha descripción

Responsabilidades de la empresa u organización de servicios NP Enterprise Inc.

La empresa de servicios NP Enterprise Inc. es responsable de: preparar la descripción y aseveración incluyendo la integridad, exactitud y método de presentación de la descripción y aseveración; proporcionar los servicios cubiertos en la descripción; establecer los objetivos de control; y diseñar, implementar y operar eficazmente los controles para lograr los objetivos de control establecidos.

Responsabilidades del auditor de servicio

Nuestra responsabilidad es expresar una opinión sobre la descripción de la empresa servicios NP Enterprise Inc. y sobre el diseño y la operación de los controles relacionados con los objetivos de control establecidos en dicha descripción, con base en nuestros procedimientos. Llevamos a cabo nuestro trabajo de conformidad con la Norma Internacional de Trabajos de Aseguramiento 3402,

"Informes de aseguramiento sobre los controles en una organización de servicio", emitida por el Consejo de Normas Internacionales sobre Auditoría y Atestiguamiento, la cual prevé que cumplamos con los requerimientos éticos, y que planifiquemos y realicemos nuestros procedimientos para obtener una seguridad razonable de que, en todos los aspectos materiales, la descripción está presentada razonablemente y los controles están diseñados adecuadamente y operan con efectividad.

Un trabajo de atestiguamiento para informar sobre la descripción, diseño y efectividad operativa de los controles en una empresa u organización de servicios implica llevar a cabo procedimientos para obtener evidencia acerca de las revelaciones en la descripción de su sistema de la organización de servicio, y en el diseño y efectividad operativa de los controles. Los procedimientos seleccionados dependen del juicio del auditor de la empresa de servicios, que incluye evaluar los riesgos acerca de que la descripción no se presente razonablemente, y que los controles no estén diseñados de manera adecuada ni que operen eficazmente. Nuestros procedimientos incluyeron pruebas de la efectividad operativa de los controles que consideramos necesarios para ofrecer seguridad razonable de que se lograron los objetivos de control establecidos en la descripción. Un trabajo de aseguramiento de este tipo también incluye evaluar la presentación general de la descripción, lo apropiado de los objetivos establecidos en ella, y la idoneidad de los criterios fijados por la empresa u organización de servicios. Consideramos que la evidencia que hemos obtenido es suficiente y apropiada para proporcionar una base para sustentar nuestra opinión.

Limitaciones de los controles en una empresa u organización de servicios

La descripción de la empresa u organización de servicios NP Enterprise Inc. está preparada para satisfacer las necesidades comunes de una amplia gama de clientes y sus auditores, y no puede,

por tanto, incluir todos los aspectos del sistema que cada cliente puede considerar importante en su entorno particular. Además, debido a su naturaleza, los controles en una empresa u organización de servicios quizá no puedan prevenir ni detectar todos los errores u omisiones en el procesamiento o el informe de transacciones. Asimismo, la proyección de cualquier evaluación de la efectividad a períodos futuros está sujeta al riesgo de que los controles en la empresa u organización de servicios puedan llegar a ser insuficientes o fallar.

Opinión

Nuestra opinión se ha formado sobre la base de los asuntos esbozados en este informe. Los criterios que utilizamos para formar nuestra opinión son los descritos en el informe de control adjunto. En nuestra opinión, respecto de todo lo importante:

- La descripción presenta razonablemente de los sistemas, como fue diseñado e implementado, durante el período comprendido entre el 01 de enero al 31 de diciembre del 2016;
- Los controles relacionados con los objetivos de control establecidos en la descripción fueron diseñados adecuadamente durante todo el período comprendido entre el 01 de enero al 31 de diciembre del 2016; y
- Los controles probados, fueron los necesarios para ofrecer seguridad razonable de que se lograron los objetivos de control establecidos en la descripción y operaron eficazmente durante todo el período comprendido entre el 01 de enero al 31 de diciembre del 2016.

Descripción de las pruebas de los controles

Los controles específicos probados y la naturaleza, duración y resultados de dichas pruebas.

Usuarios previstos y propósito

Este informe y la descripción de las pruebas de los controles que se incluyen en las están dirigidos únicamente para los clientes que han utilizado en los sistemas de la empresa de servicios NP Enterprise Inc., y para sus auditores, que tienen conocimiento suficiente para considerarlo, junto con otra información que incluye datos sobre los controles operados por los propios clientes, al evaluar los riesgos de error material de los estados financieros de los clientes.

Hector Alejandro Salgado Palacios

Contador Público Autorizado

5.4.9.4. Carta de observaciones y recomendaciones del control interno sobre el sistema de información computarizado

15 de diciembre de 2016

Lic. Rigoberto Lopez

Gerente General

NP Enterprise Inc.

Managua, Nicaragua

Estimado licenciado Alomar:

En la planeación y ejecución de nuestra auditoría de aseguramiento de NP Enterprise Inc. por el año que terminó el 31 de diciembre de 2016, obtuvimos una comprensión de los sistemas de contabilidad y de control interno que utilizan sistemas de información computarizados, para determinar la naturaleza, alcance y oportunidad de nuestros procedimientos de auditoría. Es importante señalar que esta examinación no ha sido diseñada para determinar la adecuación del control interno para fines de la administración.

Nuestras observaciones y recomendaciones se presentan en los siguientes anexos:

- Resumen ejecutivo en el que se describen los principales hallazgos detectados en el ambiente de sistema de información computarizado.
- Informe detallado de las recomendaciones del período en revisión.

Esta carta es sólo para información y uso de la Junta Directiva, así como la administración superior de NP Enterprise Inc. y no debe ser utilizado para ningún otro propósito.

Atentamente,

Michael Tejeda Valenzuela

Contador Público Autorizado

5.4.9.5. Ambiente general de los sistemas

5.4.9.5.1. Resumen ejecutivo

Las políticas de seguridad, sus objetivos, fundamentos y responsabilidades, constituyen un marco de protección a los recursos, sistemas e información contra riesgos accidentales o intencionales en lo referente a la integridad, disponibilidad y confidencialidad de la información. La arquitectura de seguridad de la Compañía debe consistir en la interrelación de un conjunto de objetivos, fundamentos, políticas y normas bajo las cuales pueden implementarse controles específicos de seguridad en función de los riesgos inherentes a un ambiente tecnológico.

Como parte de la comprensión de los sistemas de contabilidad y de control interno que utilizan sistemas de información computarizados, necesarios para determinar la naturaleza, alcance y oportunidad de nuestros procedimientos de auditoría sobre los estados financieros de NP Enterprise Inc. por el año que terminó el 31 de diciembre de 2016, revisamos los controles del departamento de informática respecto a los siguientes factores:

- Organización y administración - Con el objetivo de analizar y evaluar las políticas, administración y estructura organizativa, procedimientos operativos y ambiente de control del área encargada de la informática de la Compañía.
- Operaciones del centro de procesamiento de datos - Con el objetivo de identificar, analizar y evaluar las tareas, procedimientos y controles dentro de la sala del computador y las áreas que dan soporte y apoyan a todas las oficinas de los usuarios.
- Controles de acceso lógico, físicos y ambientales - Con el objetivo de analizar y evaluar el sistema de controles diseñado para resguardar de daños a la instalación frente a amenazas accidentales, intencionales y naturales, uso indebido o destrucción.
- Continuidad de las operaciones - Con el objetivo de analizar y evaluar las políticas y los procedimientos adecuados a la planificación de contingencias para asegurar la capacidad de la Compañía para responder eficazmente ante desastres y otras situaciones de emergencia.
- Adquisición y mantenimiento de software base - Con el objetivo de analizar y evaluar las políticas y procedimientos relacionados a la seguridad y control de adquisición y mantenimiento del software base (sistemas operativos, manejadores de bases de datos, etc.).
- Desarrollo, adquisición y mantenimiento de software aplicativo - Con el objetivo de identificar, analizar y evaluar la metodología utilizada para el desarrollo, adquisición y mantenimiento de aplicaciones.

- Evaluación de los sistemas aplicativos - Con el objetivo de identificar, analizar y evaluar fortalezas, debilidades, eficiencia y efectividad de los componentes en los sistemas aplicativos existentes.

A continuación, se presenta un resumen de las observaciones identificadas:

5.4.9.5.2. Informe detallado de recomendaciones

Con el fin de mejorar y fortalecer el control interno sobre los sistemas de información computarizados de NP Enterprise Inc. se presentan las recomendaciones a las debilidades observadas durante nuestra revisión:

Área: Seguridad Lógica

- Nombre del Componente: Acceso de los usuarios a sistemas, sistemas operativos y bases de datos.

Hallazgo: No existe validación alguna para acceder al Sistema Operativo o a los archivos de las PCs, a excepción de la PC del encargado de Operaciones, la empresa no cuenta con base de datos de ningún tipo.

Recomendación: Se recomienda poner contraseñas en el inicio del sistema operativo y en el BIOS de cada PC, actualmente no se cuenta con una base de datos en la empresa, pero al implementarse lo recomendable es tener un administrador que sea el responsable de la contraseña del BD.

- Nombre del Componente: Acceso de los usuarios a programas y archivos.

Hallazgo: No existe ninguna validación de usuario en las PC, se puede tener acceso a cualquier archivo sin necesidad de usuario y contraseña, también cada PC es usada por más de un usuario.

Recomendación: Se recomienda que los archivos estén cifrados para los usuarios que no tienen acceso a ellos, poniendo contraseña a carpetas en PCs donde se maneje información delicada de la empresa.

- Nombre del Componente: Disposición de sistemas alternos en caso de fallos.

Hallazgo: Falta de un servidor para el sistema TCO, el que está instalado en una PC con mayores requerimientos que las demás PC para poder funcionar como servidor.

Recomendación: Se recomienda mantener un sistema en caso de fallos, un sistema menos potente pero que trabaje similar al TCO ya que ese es el sistema de aforo.

Área: Seguridad Física

- Nombre del Componente: Control de accesos de los usuarios a los equipos.

Hallazgo: Solo los trabajadores del área de operaciones tienen acceso a los equipos de esta misma área.

Recomendación: Se recomienda mantener una lista para el control de quien acceda a los equipos, así como tener una lista de los usuarios autorizados de los equipos y el horario en el que estos tienen derecho a ocupar los equipos, en una mejor instancia mantener un control electrónico por medio de tarjetas que identifiquen a los empleados según cargo.

- Nombre del Componente: Informes de accesos y visitas a las instalaciones.

Hallazgo: No existe un control tangible de quienes entran o salen del área de operaciones, que es donde se encuentran los procesos más críticos de la empresa, para poder

entrar se necesita la autorización del gerente, pero el control es verbal, no se lleva registro o documentación de visitas, para acceder al centro.

Recomendación: Se recomienda establecer un horario de visita a las instalaciones y mantener un control de parte del encargado para poder ingresar, así como revisión de las personas que quieran ingresar a las instalaciones, además del permiso del gerente, para que exista constancia física o digital de que personas entraron a las instalaciones y a qué hora.

- Nombre del Componente: Inventario de equipos y software

Hallazgo: Falta de automatización de algunos procesos que podrían ser más rápidos y menos tediosos, como es el inventario de los equipos dados de baja y puestos en bodega, el control de estos se lleva a mano.

Recomendación: Se recomienda que el inventario se lleve de manera digitalizada, actualmente se lleva de manera física, pero es más eficiente de manera digital, alojando todo el inventario en un pequeño BD en un servidor

- Nombre del Componente: Revisión de la red (Factor ambiental, Físico y humano).

Hallazgo: El cableado proporcionado por el ISP (Internet Servicie Proveer) que en este caso es DATATEX, que conforma la red entera posee muy poca estandarización, el cableado instalado es meramente plano compuesto casi en su totalidad por cable UTP cat. 5e.

Recomendación: Se recomienda mejorar las condiciones del cable de red que conecta la antena satelital al Router de la empresa, para que este no esté suelto, se pretende que esto se realice por medio de cintas de seguridad, amarradas en la antena, también se recomienda cumplir con la norma de la ISO y mantener las conexiones y equipos de telecomunicaciones a más de 10 metros de distancia.

Área: Respaldos y Planes de Contingencia

- Nombre del Componente: Respaldo de Información crítica.

Hallazgo: Falta de digitalización de sus documentos, existe respaldo solo en físico, por lo tanto, no están preparados para ninguna eventualidad.

Recomendación: Se recomienda comprar un servidor para poder almacenar los datos críticos en una base de datos.

- Nombre del Componente: Plan de continuidad.

Hallazgo: Carecen de planes de reanudación de operaciones y planes en caso de desastres. Como se puede observar esto es un punto de debilidad en la empresa porque mediante estos se asegura que la empresa seguirá ofreciendo su servicio sin importar las condiciones.

Recomendación: Se recomienda crear planes en caso de fallas parciales o totales de los sistemas de la empresa, para poder garantizar el seguimiento de operaciones para la misma. Además, se recomienda contar con un plan de contingencia para poder recuperar y reanudar sus operaciones sin importar los acontecimientos.

- Nombre del Componente: Plan de Contingencia.

Hallazgo: Carecen de planes de reanudación de operaciones y planes en caso de fallo total o parcial de sus sistemas como se puede observar esto es un punto de debilidad en la empresa porque mediante es tos se asegura que la empresa seguirá ofreciendo su servicio sin importar las condiciones.

Recomendación: Se recomienda tener un plan de mantenimiento, para mantener informado al personal encargado las tareas a realizar, para que tanto directivos como demás gente involucrada en el mantenimiento esté enterada de lo que se hace y se cercioren de que el

mantenimiento se realiza de manera adecuada y a como establece el plan para mantener control y orden.

- Nombre del Componente: Plan de Mantenimiento de Hardware y Software.

Hallazgo: No se cuenta con un plan sólido de mantenimiento de hardware, se realiza 3 veces durante el año, de dos maneras preventivas y correctivas y el de software solo de manera correctiva, ambos realizados por terceros.

Recomendación: Se recomienda la creación formal de un plan de mantenimiento y establecer los procedimientos de las tareas a realizar. planes y procedimientos que deberán ser dados a conocer a todos los empleados, a cerca del correcto uso de los equipos informáticos, para optimizar los servicios de mantenimiento contratados por la empresa, además se recomienda llevar un registro detallado de las actividades que se realizan en cada tarea.

Área: Documentación de Hardware y Software

- Nombre del Componente: Documentación de los sistemas utilizados para los servicios utilizados para los servicios de la empresa.

Hallazgo: No existe ninguna documentación en cuanto a diagramas y/o esquemas de los servicios utilizados por la empresa, de red o de software.

Recomendación: Se recomienda a la empresa diagramar y esquematizar el software que posea, así mismo realizarlo con su red en uso.

5.4.9.5.3. Resultado

Como resultado de la auditoría podemos revelar que se ha cumplido con evaluar cada uno de los controles plasmados en el plan de auditoría, la auditoría revelo que controles implementados no se aplicaron en forma adecuados.

Evaluando el área importante de la empresa como es el de tecnología, se evidencia que falta un manejo más amplio y exhaustivo del ambiente de TI, así mismo sucede con algunas

áreas de la empresa que no está automatizadas, la auditoría realizada debe tomarse como una guía para llevar en perfecta armonía del ambiente de TI con la misión del negocio, siguiendo con los resultados de auditoria consideramos que la empresa no tiene implementado los controles necesarios para el resguardo de la información, de igual forma muchos de los procesos de la empresa deberían ser automatizados como: el proceso de inventario, el proceso contable.

La empresa actualmente se deberá plantear en reestructurar la gestión de TI, para aumentar y mejorar su capacidad en materia de TI, se tienen controles en algunas áreas estrictos y en otras áreas no tan estrictos, por el momento la empresa se encuentra en dirección junto a TI para satisfacer las necesidades del cliente, la automatización no es completa y la adquisición para la mejora de los servicios de TI está pensada muy en el futuro.

Adicionalmente se sugiere a la empresa, realizar las tareas de actualización y mantenimiento necesarias, con énfasis en el área técnica y de tecnología, las que son esenciales para el buen funcionamiento de la empresa y para el cumplimiento de los objetivos establecidos.

Cabe destacar que es de gran importancia que la empresa contrate personal capacitado para el desarrollo de sus sistemas teniendo en cuenta los marcos normativos de información, es decir, que no adquieran sistemas enlatados, porque un sistema desarrollado internamente sería único y acorde a las necesidades de la organización.

VI. Conclusiones

Para culminar este trabajo hacemos énfasis en la importancia de este tema para el aprendizaje del estudiante, realizando el reconocimiento general de recursos y entornos de TI en la entidad.

También identificando los procesos que son abarcados en el sistema de control interno, su estandarización y el cumplimiento de los mismos.

Verificando si el ambiente de control en TI cumple con las regulaciones y requerimientos de los marcos normativos aplicables, las disposiciones y reglamentos que contribuyan a la creación e implementación de los sistemas contables

Y emitiendo recomendaciones necesarias para la prevención y mitigación de posibles riesgos que pongan en peligro la veracidad de la información y la continuidad de la entidad.

Finalmente, evaluando el sistema de control interno de la Tecnología de la Información de NP Enterprise Inc. utilizado para garantizar la veracidad, confidencialidad, confiabilidad y disponibilidad de la información financiera y no financiera al 31 de diciembre 2016 mediante la aplicación de la ISAE 3402.

VII. Bibliografía

Arens, A. A., Elder, R. J., & Beasley, M. S. (2007). *Auditoría. Un enfoque integral* (Décimo primera ed.). Estado de México, Naucalpan de Juárez, México: Pearson educación. Recuperado el 15 de Octubre de 2017

Auditoría y Control de Sistemas e Informática. (2008).

Bautista, J. (2010). *Auditoría en Informática.*

Cervantes, R. (2011). *Administración de centro de cómputo: Seguridad Lógica.*

Hernández Salguera, J. (2011). *Auditoría Informática.* Monográfico, Universidad Autónoma del Estado de Hidalgo, Sistemas computacionales, Hidalgo. Recuperado el 15 de 10 de 2017

International Federación of accountants. (2010). Manual de Pronunciamientos Internacionales. En *Manual de Pronunciamientos Internacionales* (Vol. 2, pág. 462). México. Recuperado el 3 de Noviembre de 2017

ISACA. (2012). *COBIT 5.* Roulling Meadows, Illinois, Estados Unidos de América: ISACA FRAMEWORKS.

Navarro, E. D. (2008). *Auditoría de Tecnologías y Sistemas de Información.* RA-MA, S.A.

VIII. ANEXOS

Br. Héctor Salgado Palacios
Br. Michael Tejeda Valenzuela

Anexo 1: Glosario

Alcance de la auditoría. - El marco o límite de la auditoría y las materias, temas, segmentos o actividades que son objeto de la misma.

Alta gerencia. -La alta gerencia está compuesta por una cantidad de personas comparativamente pequeña y es la responsable de administrar toda la organización. Estas personas reciben el nombre de ejecutivos. Establecen las políticas de las operaciones y dirigen la interacción de la organización con su entorno.

Amenaza. - Cualquier aspecto o escenario que pueda ocasionar que un riesgo se convierta en incidente, o sea, que llegue a realizarse.

Archivos de sistema. - Son aquellos archivos de uso exclusivo del sistema operativo. Estos archivos no pueden ser eliminados normalmente por el usuario o el sistema le advierte que se dispone a eliminar un fichero necesario para su correcto funcionamiento.

Auditor. - Persona que efectúa una auditoría.

Auditoría. - Examen de las operaciones de una empresa, realizado por especialistas ajenos a ella y con objetivos de evaluar la situación de la misma.

Auditoría de sistema. Es la revisión que se dirige a evaluar los métodos y procedimientos de uso en una entidad, con el propósito de determinar si su diseño y aplicación son correctos; y comprobar el sistema de procesamiento de información como parte de la evaluación de control interno; así como para identificar aspectos susceptibles de mejorarse o eliminarse.

Auditoría de tecnologías de la información. Consiste en el examen de las políticas, procedimientos y utilización de los recursos informáticos; confiabilidad y validez de la

información, efectividad de los controles en las áreas, las 10 aplicaciones, los sistemas de redes y otros vinculados a la actividad informática.

Bases de Datos. - Colección de datos pertenecientes a un mismo contexto, organizada de tal modo que el ordenador pueda acceder rápidamente a ella. Una base de datos relacionar, es aquella en la que las conexiones entre los distintos elementos que forman la base de datos están almacenadas explícitamente con el fin de ayudar a la manipulación y el acceso a éstos.

Bitácoras. - Es como el "diario" de algunos programas donde se graban todas las operaciones que realizan, para posteriormente abrirlos y ver qué es lo que ha sucedido en cada momento.

Capacitación. - Toda acción organizada y evaluable que se desarrolla en una empresa para: modificar, mejorar y ampliar los conocimientos; habilidades y actitudes del personal, generando un cambio positivo en el desempeño de sus tareas.

COBIT: Control Objetives for Information and related Technology (Objetivos de Control para Tecnología de la Información y Relacionadas).

Cliente. - Cliente o “programa cliente”, es aquel programa que permite conectarse a un determinado sistema, servicio o red.

Cliente-Servidor. - Se denomina así, al binomio consistente en un programa cliente que consigue datos de otro llamado servidor, sin tener que estar obligatoriamente ubicados en el mismo ordenador. Esta técnica de consulta 'remota' se utiliza frecuentemente en redes como 'Internet'.

Eficacia. - Capacidad de lograr el efecto que se desea o se espera.

Eficiencia. - Conjunto de atributos, que se refieren a las relaciones entre el nivel de rendimiento del software y, la cantidad de recursos utilizados bajo unas condiciones predefinidas.

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.

Evaluación. - Es el proceso de recolección y análisis de información y, a partir de ella, presentar las recomendaciones que facilitarán la toma de decisiones.

Elemento del modelo. - Es una abstracción destacada del sistema que está siendo modelado.

Evaluación de Riesgo. - Es el proceso utilizado para identificar y evaluar riesgos y su impacto potencial.

Evidencia. - Es toda información que utiliza el AI, para determinar, si el ente o los datos auditados siguen los criterios u objetivos de la auditoría.

Evidencia de auditoría. - las pruebas que obtiene el auditor, durante la ejecución de la auditoría, que hace patente y manifiesta la certeza o convicción, sobre los hechos o hallazgos, que prueban y demuestran claramente éstos, con el objetivo de fundamentar y respaldar sus opiniones y conclusiones.

Estándares: Es una especificación o modelos que regulan la realización de ciertos procesos o la fabricación de componentes para garantizar la interoperabilidad.

Hallazgos. Son evidencias, como resultado de un proceso de recopilación y síntesis de información: la suma y la organización lógica de información, relacionada con la entidad, actividad, situación o asunto que se haya revisado o evaluado, para llegar a conclusiones al

respecto o para cumplir alguno de los objetivos de la auditoría. Sirven de fundamento a las conclusiones del auditor y, a las recomendaciones que esta fórmula para que se adopten las medidas correctivas.

Herramienta. - Es el conjunto de elementos físicos utilizados para llevar a cabo las acciones y pasos definidos en la técnica.

Herramienta de Control. - Son elementos de software, que permiten definir uno o varios procedimientos de control, para cumplir una normativa y un objetivo de control.

Herramientas de Software de Auditoría. - Son programas computarizados, que pueden utilizarse para brindar información para uso de auditoría.

Informática. - Ciencia que estudia el tratamiento automático de la información en computadoras, dispositivos electrónicos y, sistemas informáticos.

Informe de Auditoría. - Es el producto final del Auditor de SI; constituye 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, conclusiones y recomendaciones.

Integridad. - Consiste en que solo los usuarios autorizados puedan variar los datos.

Irregularidades. - Son las violaciones intencionales a una política gerencial establecida, declaraciones falsas deliberadas u omisión de información del área auditada o de la organización.

Infraestructura tecnológica. - Conjunto de elementos de hardware (servidores, puestos de trabajo, redes, enlaces de telecomunicaciones, etc.), software (sistemas operativos, bases de datos, lenguajes de programación, herramientas de administración, etc.) y servicios (soporte técnico, seguros, comunicaciones, etc.); que en conjunto dan soporte a las aplicaciones (sistemas informáticos) de una empresa. 13

Jerarquía. - Es la disposición de personas, animales o cosas, en orden ascendente o descendente, según criterios de clase, poder, oficio, categoría, autoridad o cualquier otro asunto que conduzca a un sistema de clasificación.

Metodología: Se refiere a los métodos de investigación que se siguen para alcanzar una gama de objetivos en una ciencia. Aun cuando el término puede ser aplicado a las artes, cuando es necesario efectuar una observación o análisis más riguroso o explicar una forma de interpretar la obra de arte. En resumen, son el conjunto de métodos que se rigen en una investigación científica o en una exposición doctrinal.

Norma. - Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción, así como el correcto desarrollo de una actividad.

Normas de auditoría: Constituyen el conjunto de reglas que deben cumplirse, para realizar una auditoría con la calidad y eficiencia indispensables.

Objetivo de la auditoría. Propósito o fin que persigue la auditoría, o la pregunta que se desea contestar por medio de aquella. Auditoría.

Objetivo de Control. - Son declaraciones sobre el resultado final deseado o propósito a ser alcanzado, mediante las protecciones y los procedimientos de control. Son los objetivos por cumplir en el control de procesos.

Ofimática. - Es el sistema informatizado que genera, procesa, almacena, recupera, comunica y presenta datos relacionados con el funcionamiento de la oficina.

Outsourcing. - Es un contrato a largo plazo de un sistema de información o proceso de negocios, a un proveedor de servicios externos.

Políticas. - Conjunto de disposiciones documentadas que regulan el comportamiento de un grupo de individuos.

Política interna. - Conjunto de normas, reglas y disposiciones que regulan el comportamiento, las responsabilidades y las restricciones del personal de una empresa.

Prevención. - Adopción de medidas encaminadas a impedir que se produzcan deficiencias físicas, mentales y sensoriales (prevención primaria) o a impedir que las deficiencias, cuando se han producido, tengan consecuencias físicas, psicológicas y sociales negativas.

Procedimientos de Control. - Son los procedimientos operativos de las distintas áreas de la empresa, obtenidos con una metodología apropiada, para la consecución de uno o varios objetivos de control y, por tanto, deben estar documentados y aprobados por la Dirección.

Procedimientos Generales de Auditoría. - Son los pasos básicos en la realización de una auditoría.

Pruebas de Cumplimiento. - Son aquellas evidencias que determinan que (proporcionan evidencia de que) los controles claves existen y que son aplicables en forma efectiva y uniforme.

Pruebas Sustantivas. - Son aquellas que implican el estudio y evaluación de la información, por medio de comparaciones con otros datos relevantes.

Resumen Ejecutivo. - Es un informe de fácil lectura, gramaticalmente correcto y breve, que presenta los hallazgos a la gerencia en forma comprensible.

Riesgo. Posibilidad de que no puedan prevenirse o detectarse errores o irregularidades importantes.

- ✓ Riesgo inherente. Existe un error que es significativo y se puede combinar con otros errores cuando no hay control.
- ✓ Riego de control. Error que no puede ser evitado o detectado oportunamente por el sistema de control interno.

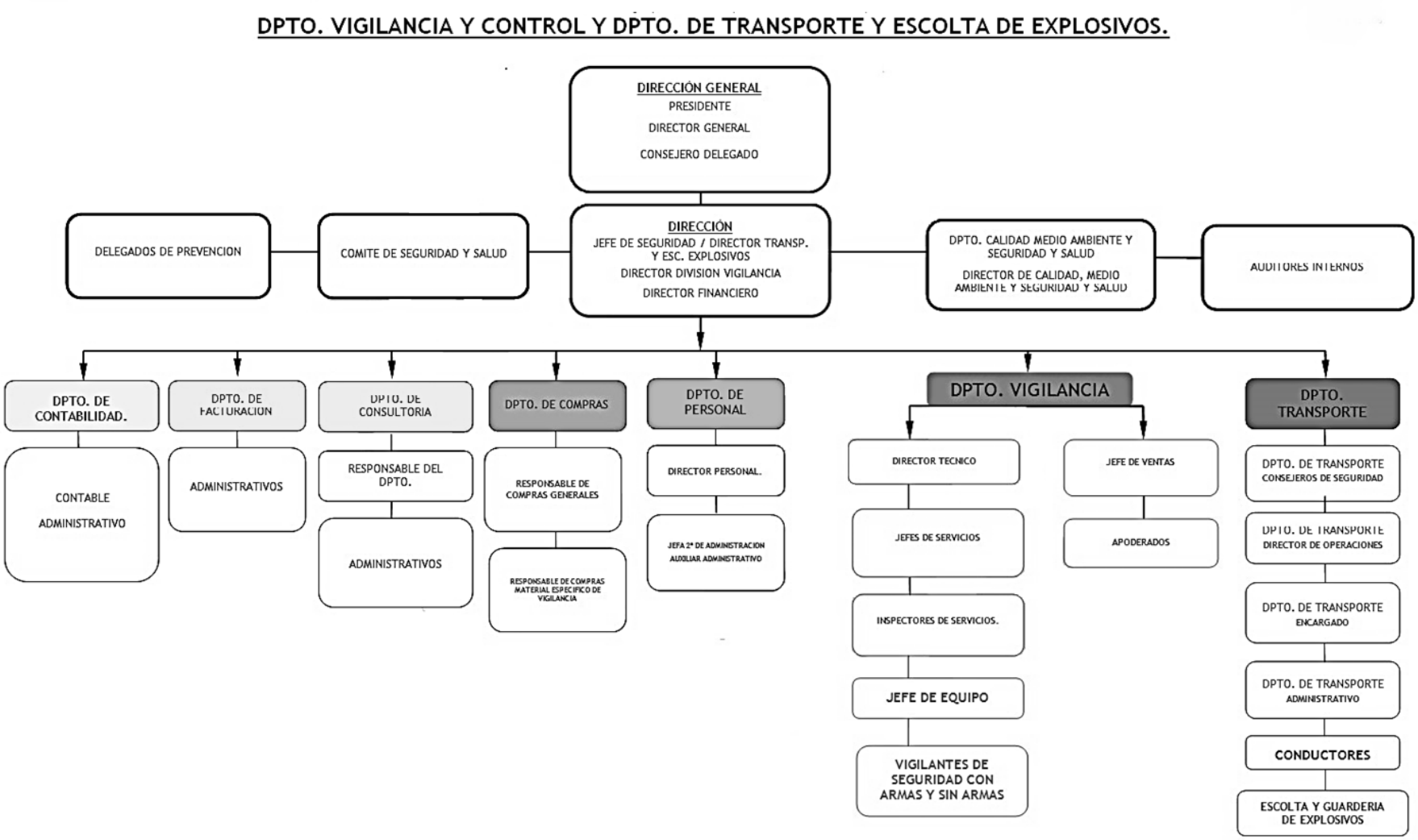
- ✓ Riesgo de detección. Se realizan pruebas exitosas a partir de un procedimiento de prueba inadecuado.

Sistema Operativo: Software de sistema, es decir, un conjunto de programas de computadora, destinado a permitir una administración eficaz de sus recursos. Comienza a trabajar cuando es cargado en memoria por un programa específico, que se ejecuta al iniciar el equipo, o al iniciar una máquina virtual y, gestiona el hardware de la máquina desde los niveles más básicos, brindando una interfaz con el usuario.

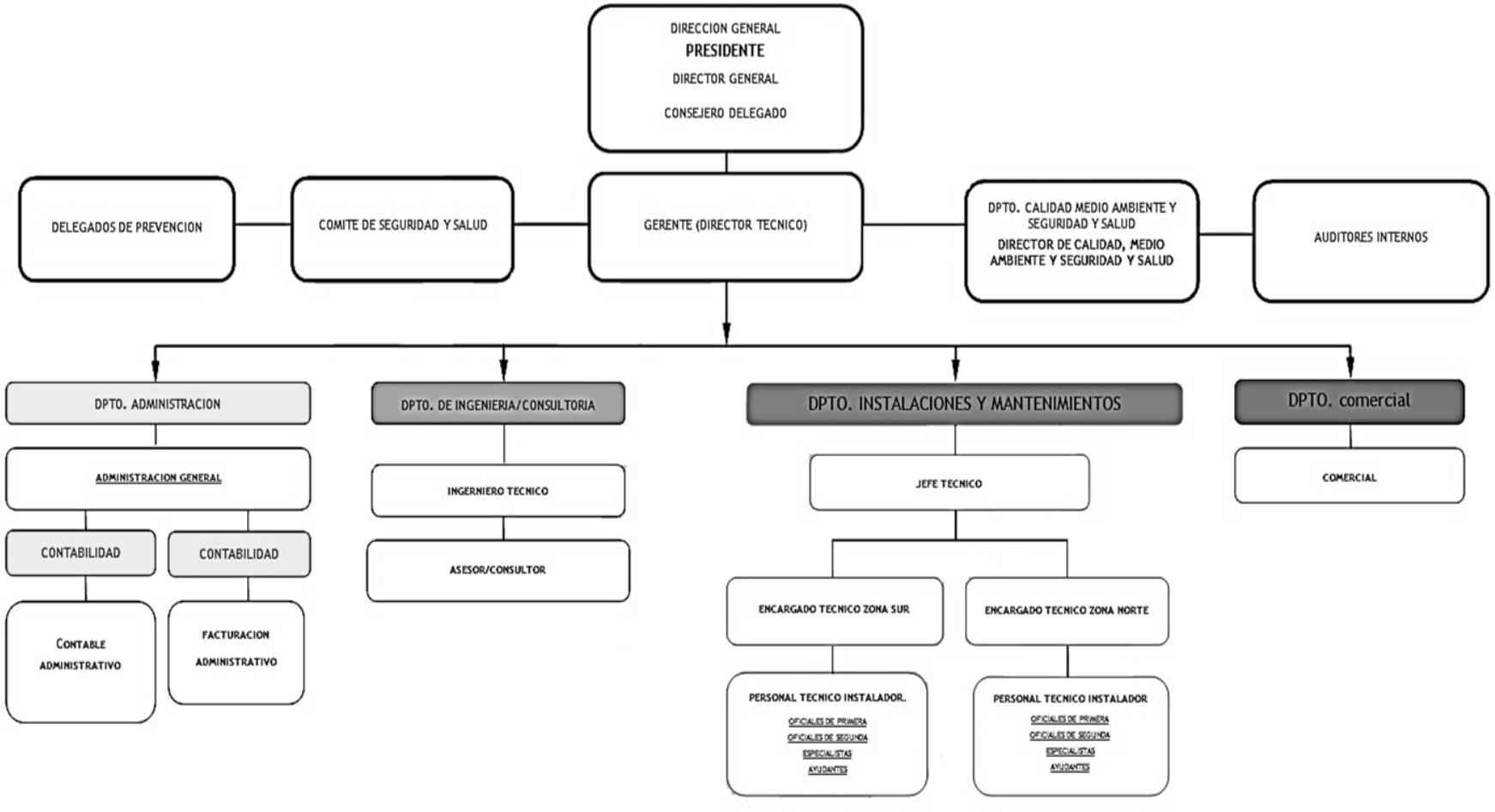
Técnicas de auditoría. Métodos que el auditor emplea, para realizar las verificaciones planteadas en los programas de auditoría, que tienen como objetivo la obtención de evidencia.

UPS: Es un dispositivo que proveen y mantiene energía eléctrica de respaldo en caso de interrupciones eléctricas o eventualidades en la línea o acometida. Adicionalmente, los UPS cumplen la función de mejorar la calidad de la energía eléctrica que llega a las cargas, como el filtrado, protección de subidas (picos de tensión), bajadas de tensión (caídas), apagones y eliminación de corrientes parasitarías como ruidos, interrupción de energía, perdida de data, etc.

Anexo 2: Estructura organizativa



DPTO. INSTALACIONES DE SISTEMAS DE SEGURIDAD Y MANTENIMIENTO.



Anexo 3: Plan de auditoría

Antecedentes

La empresa NP Enterprise Inc., empresa que se dedica a la seguridad física, las actividades que se realizan en esta empresa son de diversos tipos tales como: venta de productos y servicios de seguridad física, electrónica, consultorías y capacitaciones, entre otros. Esta empresa como parte de su crecimiento hace uso del ambiente de TI para sistematizar las áreas del negocio y así ofrecer servicio de calidad a sus clientes.

Uno de los recursos tecnológicos disponibles en las empresas de seguridad es la red de datos que opera en las diferentes sedes y que generalmente se encuentra certificada bajo la norma de la IEEE\EIA\TIA, las cuales se deben cumplir estrictamente.

Objetivos

Objetivo general: Realizar la revisión y verificación del cumplimiento de normas mediante una auditoría a la infraestructura física de la red de datos en una de las instituciones educativas.

Objetivos específicos:

- Planificar la auditoría que permita identificar las condiciones actuales de la red de datos de la institución educativa.

- Aplicar los procesos de auditoría teniendo en cuenta el modelo estándar de auditoría COBIT como herramienta de apoyo en el proceso inspección de la red de datos de la institución educativa.
- Identificar las soluciones para la construcción de los planes de mejoramiento a la red de la institución educativa de acuerdo a los resultados obtenidos en la etapa de aplicación del modelo de auditoría.

Alcance y delimitación: La presente auditoria pretende identificar las condiciones actuales del hardware, la red de datos y eléctrica de la institución educativa, con el fin de verificar el cumplimiento de normas y la prestación del servicio de internet para optimizar el uso de los recursos existentes para mejorar el servicio a los usuarios.

Los puntos a evaluar serán los siguientes:

De las instalaciones físicas se evaluará:

- Instalaciones eléctricas
- Instalación cableada de la red de datos
- Sistemas de protección eléctricos

Seguridad de acceso físico a las instalaciones

De equipos o hardware se evaluará:

- Inventarios de hardware de redes y equipos
- Mantenimiento preventivo y correctivo de equipos y redes

  Hojas de vida de los equipos de cómputo y redes
- Los programas de mantenimiento de los equipos de cómputo y redes
- Revisión de informes de mantenimiento

- Personal encargado de mantenimiento

Obsolescencia de la tecnología

Metodología: Para el cumplimiento de los objetivos planteados en la auditoría, se realizarán las siguientes actividades:

Investigación preliminar: visitas a la institución para determinar el estado actual de la organización, entrevistas con administradores y usuarios de las redes para determinar posibles fallas, entrevistas con administrador y usuarios para determinar la opinión frente al hardware existente y obsolescencia de equipos.

Recolectar información: Diseño de formatos de entrevistas, diseño de formatos para listas de chequeo, diseño de formatos para cuestionarios, diseño del plan de pruebas, selección del estándar a aplicar, elaboración del programa de auditoría, distribución de actividades para los integrantes del grupo de trabajo.

Aplicación de instrumentos: Aplicar entrevistas al administrador y usuarios, aplicar listas de chequeo para verificar controles, aplicar cuestionarios para descubrir nuevos riesgos y conformar los que han sido detectados anteriormente.

Ejecución de las pruebas: ejecutar las pruebas para determinar la obsolescencia del hardware, ejecutar pruebas sobre la red, ejecutar pruebas para comprobar la correspondencia de los inventarios con la realidad.

Realizar el proceso de análisis y evaluación de riesgos: elaborar el cuadro de vulnerabilidades y amenazas a que se ven enfrentados, determinar los riesgos a que se ven expuestos, hacer la evaluación de riesgos, elaborar el mapa o matriz de riesgos.

Tratamiento de riesgos: determinar el tratamiento de los riesgos de acuerdo a la matriz de riesgos, proponer controles de acuerdo a la norma de buena práctica aplicada, definir las posibles

soluciones

Dictamen de la auditoría: Determinar el grado de madurez de la empresa en el manejo de cada uno de los procesos evaluados, medir el grado de madurez de acuerdo a los hallazgos detectados en cada proceso.

Informe final de auditoría: Elaboración del borrador del informe técnico de auditoría para confrontarlo con los auditados, elaboración del informe técnico final, elaboración del informe ejecutivo, organización de papeles de trabajo para su entrega.

Normativa Aplicable

La normativa utilizada en el desarrollo de la auditoria es COBIT 5.0

Este modelo incluye un modelo de referencia de procesos que define y describe en detalle varios procesos de gobierno y de gestión. Dicho modelo representa todos los procesos que normalmente encontramos en una empresa relacionados con las actividades de TI,

Este proporciona un modelo de referencia común entendible para las operaciones de TI y los responsables de negocio. El modelo de proceso propuesto es un modelo completo e integral, pero no constituye el único modelo de procesos posible. Cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación particular.

La incorporación de un modelo operacional y un lenguaje común para todas las partes de la empresa involucradas en las actividades de TI es uno de los pasos más importantes y críticos hacia el buen gobierno. Adicionalmente proporciona un marco para medir y vigilar el rendimiento de TI, proporcionar garantía de TI, comunicarse con los proveedores de servicio e integrar las mejores prácticas de gestión.

El modelo de referencia de procesos de COBIT 5 divide los procesos de gobierno y de gestión de la TI empresarial en dos dominios principales de procesos:

Gobierno: contiene cinco procesos de gobierno; dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión (EDM).

Gestión: contiene cuatro dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar.

Estos dominios son una evolución de la estructura de procesos y dominios de COBIT 4.1. Los nombres de estos dominios han sido elegidos de acuerdo a estas designaciones de áreas principales, pero contienen más verbos para describirlos:

Alinear, Planificar y Organizar (Align, Plan and Organise, APO)

Construir, Adquirir e Implementer (Build, Acquire and Implement, BAI)

Entregar, dar Servicio y Soporte (Deliver, Service and Support, DSS)

Supervisar, Evaluar y Valorar (Monitor, Evaluate and Assess, MEA)

y supervisar (Plan, Build, Run and Monitor - PBRM), y proporciona cobertura de extremo a extremo de las TI

Cada dominio contiene un número de procesos. A pesar de que, según hemos descrito antes, la mayoría de los procesos requieren de actividades de “planificación”, “implementación”, “ejecución” y “supervisión”, bien en el propio proceso, o bien en la cuestión específica a resolver (como p. ej. calidad, seguridad), están situados en dominios de acuerdo con el área más relevante de actividad cuando se considera la TI a un nivel empresarial.

Detalle de procesos a ejecutar

El proceso de realización de esta auditoría se acordó de manera formal con la alta dirección de la empresa NP Enterprise Inc., en una reunión donde se convino entre el gerente general y los auditores, el área a auditar, los límites y alcances de la misma, visitas y tiempo de evaluación.

Las áreas a evaluar fueron analizadas mediante los procedimientos y evaluando el riesgo por área implementando una matriz de riesgo y los procedimientos del Estándar de COBIT 5.0 tomadas en distintas áreas realizando y el cual establece cuatro dominios. Debido al tiempo de ejecución, el análisis de esta auditoría se basará en los siguientes dominios: Adquisición e implementación (Build, Adquisition and implementation (BAI)), Entregar, dar servicios y soporte (Delivery Service and Support (DSS)), así mismo de estos dos dominios no se usarán todos los subprocesos efectuando una guía de implementación de componentes y procesos

Recursos:

- **Humanos:** La auditoría se llevará a cabo por el grupo de auditores especializados en redes de datos con la asesoría metodológica de un Ingeniero Auditor.
- **Físicos:** Instalaciones de la institución educativa, aulas de informática y dispositivos de red.
- **Tecnológicos:** equipos de cómputo, software instalado para la red, cámara digital, Intranet institución educativa

Presupuesto:

Ítem	Valor
Útiles y Papelería	C$ 20.000
Equipos de Oficina.	C$ 80.000
Medios de almacenamiento magnético como: 1 caja de CD, 2 USB	C$ 20.000
Gastos generales: Cafetería, imprevistos, transporte, etc.	C$ 15.000
Pago de Honorarios (40000 x c/au)	C$ 320,000
Total Presupuesto	C$ 455.000

Cronograma

Actividad		Mes 1				Mes 2				Mes 3			
		1	2	3	4	1	2	3	4	1	2	3	4
Planificar la auditoría	Estudio Preliminar	■	■										
	Determinación de Áreas Críticas de Auditoria		■										
Aplicar el modelo de auditoria	Elaboración de Programa de Auditoria			■	■	■							
	Evaluación de Riesgos					■	■						
	Ejecución de Pruebas y Obtención de Evidencias							■	■	■			
Construir los planes de mejoramiento	Elaboración de Informe										■	■	
	Sustentación de Informe												■

_____ _____

Hector Salgado P. Michael Tejeda V.

CPA CPA

Anexo 4: Cuestionarios de Control Interno

Lista de chequeo		**R/PT**		
Cuestionario de Control		**LC1**		
Dominio	Construcción, Adquisición e Implementación			
Proceso	BAI03: Gestionar la Identificación y la Construcción de Soluciones			
Objetivo de Control	Evaluación de Nuevo Hardware			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Se cuenta con un inventario de todos los equipos que integran la división?				
¿Con cuanta frecuencia se revisa el inventario?				
¿Se posee de bitácoras de fallas detectadas en los equipos?				
Características de la bitácora (señale las opciones).				
¿La bitácora es llenada por personal especializado? ¿Señala fecha de detección de la falla? ¿Señala fecha de corrección de la falla y revisión de que el equipo funcione correctamente? ¿Se poseen registros individuales de los equipos? ¿La bitácora hace referencia a hojas de servicio, en donde se detalla la falla, y las causas que la originaron, así como las refacciones utilizadas?				
¿Se lleva un control de los equipos en garantía, para que a la finalización de ésta, se integren a algún programa de mantenimiento?				
¿Se cuenta con servicio de mantenimiento para todos los equipos?				
¿Con cuanta frecuencia se realiza mantenimiento a los equipos?				
¿Se cuenta con procedimientos definidos para la adquisición de nuevos equipos?				
¿Se tienen criterios de evaluación para determinar el rendimiento de los equipos a adquirir y así elegir el mejor?				
Documentos probatorios presentados:				

LISTA DE CHEQUEO 2

		R/PT		
Cuestionario de Control		**LC2**		
Dominio	Construcción, Adquisición e Implementación			
Proceso	BAI03: Gestionar la Identificación y la Construcción de Soluciones			
Objetivo de Control	Mantenimiento Preventivo para Hardware			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**

¿Se lleva un control de los equipos en garantía, para que a la finalización de ésta, se integren a algún programa de mantenimiento?			
¿Se cuenta con servicio de mantenimiento para todos los equipos?			
¿Con cuanta frecuencia se realiza mantenimiento a los equipos?			
¿Se cuenta con procedimientos definidos para la adquisición de nuevos equipos?			
¿Se tienen criterios de evaluación para determinar el rendimiento de los equipos a adquirir y así elegir el mejor?			
Documentos probatorios presentados:			

LISTA DE CHEQUEO 3

		R/PT		
Lista de chequeo		**LC3**		
Dominio	Entrega de Servicios y Soportes			
Proceso	DSS01: Gestión de Operaciones.			
Objetivo de Control	Escolta de Visitantes			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Las instalaciones fueron diseñadas o adaptadas específicamente para funcionar como una oficina de tecnología?				
¿Se tiene una distribución del espacio adecuada, de forma tal que facilite el trabajo y no existan distracciones?				
¿Existe suficiente espacio dentro de las instalaciones de forma que permita una circulación fluida?				
¿Existen lugares de acceso restringido?				
¿Se cuenta con sistemas de seguridad para impedir el paso a lugares de acceso restringido?				
¿Se cuenta con sistemas de emergencia como son detectores de humo, alarmas, u otro tipo de censores?				
¿Existen señalizaciones adecuadas en las salidas de emergencia y se tienen establecidas rutas de evacuación?				
¿Se tienen medios adecuados para extinción de fuego en el unidad de cómputo?				
¿Se cuenta con iluminación adecuada y con iluminación de emergencia en casos de contingencia?				
¿Se tienen sistemas de seguridad para evitar que se sustraiga equipo de las instalaciones?				
¿Se tiene un lugar asignado para papelería y utensilios de trabajo?				
¿Son funcionales los muebles instalados dentro del centro de cómputo: cintoteca, Discoteca, archiveros, mesas de trabajo, etc?				
¿Existen prohibiciones para fumar, consumir alimentos y bebidas?				
¿Se cuenta con suficientes carteles en lugares visibles que				

recuerdan estas prohibiciones?			
¿Con cuanta frecuencia se limpian las instalaciones?			
¿Con cuanta frecuencia se limpian los ductos de aire y la cámara de aire que existe debajo del piso falso (si existe)?			
Documentos probatorios presentados:			

LISTA DECHEQUEO 4

		R/PT		
Lista de chequeo		**LC4**		
Dominio	Entrega de Servicios y Soportes			
Proceso	Protección contra Factores Ambientales			
Objetivo de Control	Controles Ambientales			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿El centro de cómputo tiene alguna sección con sistema de refrigeración?				
¿Con cuanta frecuencia se revisan y calibran los controles ambientales?				
¿Se tiene contrato de mantenimiento para los equipos que proporcionan el control ambiental?				
¿Se tienen instalados y se limpian regularmente los filtros de aire?				
¿Con cuanta frecuencia se limpian los filtros de aire?				
¿Se tiene plan de contingencia en caso de que fallen los controles ambientales?				
Documentos probatorios presentados:				

LISTA DE CHEQUEO 5

		R/PT		
Lista de chequeo		**LC5**		
Dominio	Entrega de Servicios y Soportes			
Proceso	DSS01: Gestionar las Operaciones			
Objetivo de Control	Suministro Ininterrumpido de Energía			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Se cuenta con instalación con tierra física para todos los equipos?				
¿La instalación eléctrica se realizó específicamente para el centro de cómputo?				
¿Se cuenta con otra Instalación dentro el centro de cómputo, diferente de la que alimenta a los equipos de cómputo?				
¿La acometida llega a un tablero de distribución?				
¿El tablero de distribución esta en la sala, visible y accesible?				

¿El tablero considera espacio para futuras ampliaciones de hasta de un 30 % (Considerando que se dispone de espacio físico para la instalación de más equipos)?			
¿La Instalación es independiente para el centro de cómputo?			
¿La misma instalación con tierra física se ocupa en otras partes del edificio?			
¿La iluminación está alimentada de la misma acometida que los equipos?			
¿Las reactancias (balastros de las lámparas) están ubicadas dentro de la sala?			
¿Los ventiladores y aire acondicionado están conectados en la misma instalación de los equipos a la planta de emergencia?			
¿Los ventiladores y aire acondicionado están conectados en la misma instalación de los equipos a los no-brake?			
¿Se cuenta con interruptores generales?			
¿Se cuenta con interruptores de emergencia en serie al interruptor general?			
¿Se cuenta con interruptores por secciones ó aulas?			
¿Se tienen los interruptores rotulados adecuadamente?			
¿Se tienen protecciones contra corto circuito?			
¿Se tiene implementado algún tipo de equipo de energía auxiliar?			
¿Se cuenta con Planta de emergencia?			
¿Se tienen conectadas algunas lámparas del centro de cómputo a la planta de emergencia?			
¿Qué porcentaje de lámparas: % están conectadas a la planta de emergencia (recomendable el 25 %)?			
Documentos probatorios presentados:			

LISTA DE CHEQUEO 6

		R/PT		
Cuestionario de Control		**LC6**		
Dominio	Entrega de Servicios y Soportes			
Proceso	Protección contra Factores Ambientales			
Objetivo de Control	Seguridad Física			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Se tienen lugares de acceso restringido?				
¿Se poseen mecanismos de seguridad para el acceso a estos lugares?				
¿A este mecanismo de seguridad se le han detectado debilidades?				
¿Tiene medidas implementadas ante la falla del sistema de seguridad?				
¿Con cuanta frecuencia se actualizan las claves o credenciales de acceso?				

¿Se tiene un registro de las personas que ingresan a las instalaciones?			
Documentos probatorios presentados:			

Anexo 5: Matriz de riesgo de componentes y procesos a auditar

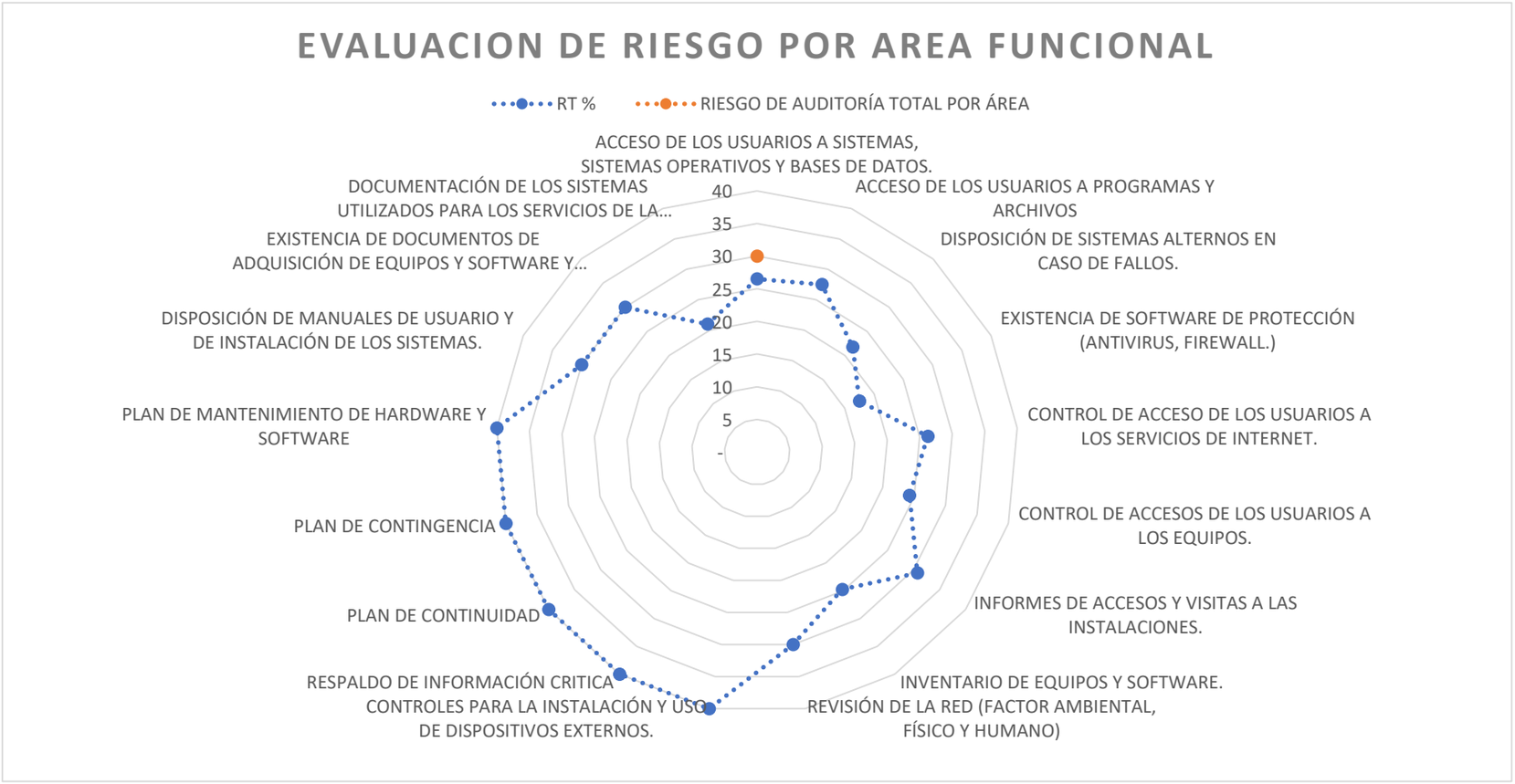
UNIDAD ADMINISTRATIVA	ACTIVIDAD	FACTORES DE RIESGO INTERNOS																																						RT	ANTECEDENTES		Verificador
		CALIDAD Y PARTICIPACIÓN				COMPLEJIDAD PROCESOS				VOLUMEN DE OPERACIONES				MANEJO Y PRESENTACION DE INFORMACION				REQUISITOS LEGALES/ REGLAMENTARIOS EXTERNO				GOBIERNO CORPORATIVO / GERENCIA				SUPERVISION Y MONITOREO				EFICIENCIA DE CONTROLES				CAMBIO IMPORTANTES EN PROCESOS, PERSONAL,O TECNOLOGIA DEL NEGOCIO				RESULTADO DE AUDITORIAS ANTERIORES					EVENTOS DE RIESGOS		
		C	I	R %	R	C	I	R %	R	C	I	R %	R	C	I	R %	R	C	I	R %	R	C	I	R %	R	C	I	R %	R	C	I	R %	R	C	I	R %	R	% 1	SI	NO	
DIVISION DE TI	ACCESO DE LOS USUARIOS A SISTEMAS, SISTEMAS OPERATIVOS Y BASES DE DATO	2	10	15%	3,00	3	15	15%	6,75	1	10	15%	1,5	2	15	10%	3	3	15	10%	4,5	1	15	5%	1	1	20	10%	2	2	15	10%	3	1	10	5%	0,5	2	15	5%	1,5	27			100%
	ACCESO DE LOS USUARIOS A PROGRAMAS Y ARCHIVOS	1	15	15%	2,25	3	15	15%	6,75	1	15	15%	2,3	2	15	10%	3	3	20	10%	6	1	15	5%	1	1	15	10%	2	2	15	10%	3	1	10	5%	0,5	2	15	5%	1,5	28			100%
	DISPOSICIÓN DE SISTEMAS ALTERNOS EN CASO DE FALLOS.	1	10	10%	1,00	1	15	10%	1,5	1	15	15%	2,3	2	15	10%	3	2	15	10%	3	1	15	10%	2	1	15	10%	2	2	20	15%	6	1	10	5%	0,5	2	15	5%	1,5	22			100%
	EXISTENCIA DE SOFTWARE DE PROTECCIÓN (ANTIVIRUS, FIREWALL.)	1	15	10%	1,50	1	15	15%	2,25	2	15	10%	3	2	10	15%	3	1	10	15%	1,5	1	15	5%	1	1	15	10%	2	2	15	10%	3	1	10	10%	1			0%	0	18			100%
	CONTROL DE ACCESO DE LOS USUARIOS A LOS SERVICIOS DE INTERNET.	3	15	15%	6,75	2	20	10%	4	1	15	5%	0,8	1	15	10%	1,5	1	15	5%	0,8	1	10	5%	1	1	20	15%	3	2	20	15%	6	1	15	15%	2,25	1	15	5%	0,75	26			100%
	CONTROL DE ACCESOS DE LOS USUARIOS A LOS EQUIPOS.	1	20	15%	3,00	1	20	15%	3	1	20	10%	2	1	20	10%	2	3	20	10%	6	1	15	5%	1	1	15	10%	2	2	15	15%	4,5	1	15	5%	0,75	1	15	5%	0,75	24			100%
	INFORMES DE ACCESOS Y VISITAS A LAS INSTALACIONES.	2	20	10%	4,00	2	20	10%	4	2	15	15%	4,5	1	20	15%	3	3	20	10%	6	1	15	10%	2	1	15	10%	2	2	20	10%	4	2	15	5%	1,5	1	15	5%	0,75	31			100%
	INVENTARIO DE EQUIPOS Y SOFTWARE.	2	20	15%	6,00	1	15	5%	0,75	1	15	20%	3	1	15	10%	1,5	3	20	10%	6	1	15	5%	1	1	15	10%	2	2	15	10%	3	1	15	10%	1,5	1	15	5%	0,75	25			100%
	REVISIÓN DE LA RED (FACTOR AMBIENTAL, FÍSICO Y HUMANO)	2	15	10%	3,00	2	15	10%	3	2	15	10%	3	2	15	10%	3	2	15	15%	4,5	2	15	10%	3	2	15	10%	3	2	15	15%	4,5	2	15	5%	1,5	2	15	5%	1,5	30			100%
	CONTROLES PARA LA INSTALACIÓN Y USO DE DISPOSITIVOS EXTERNOS.	2	20	10%	4,00	2	20	15%	6	2	20	10%	4	2	20	10%	4	2	20	15%	6	2	20	10%	4	2	20	10%	4	2	20	10%	4	2	20	5%	2	2	20	5%	2	40			100%
	RESPALDO DE INFORMACIÓN CRITICA	2	20	15%	6,00	2	20	10%	4	2	20	10%	4	2	20	10%	4	2	20	15%	6	2	20	10%	4	2	20	10%	4	2	20	10%	4	2	20	5%	2	2	20	5%	2	40			100%
	PLAN DE CONTINUIDAD	2	20	10%	4,00	2	20	10%	4	2	20	10%	4	2	20	10%	4	2	20	15%	6	2	20	10%	4	2	20	10%	4	2	20	15%	6	2	20	5%	2	2	20	5%	2	40			100%
	PLAN DE CONTINGENCIA	2	20	15%	6,00	2	20	15%	6	2	20	10%	4	2	20	10%	4	2	20	10%	4	2	20	10%	4	2	20	10%	4	2	20	10%	4	2	20	5%	2	2	20	5%	2	40			100%
	PLAN DE MANTENIMIENTO DE HARDWARE Y SOFTWARE	2	20	10%	4,00	2	20	10%	4	2	20	10%	4	2	20	10%	4	2	20	15%	6	2	20	10%	4	2	20	10%	4	2	20	15%	6	2	20	5%	2	2	20	5%	2	40			100%
	DISPOSICIÓN DE MANUALES DE USUARIO Y DE INSTALACIÓN DE LOS SISTEMAS.	2	15	15%	4,50	2	15	10%	3	2	15	10%	3	2	15	10%	3	2	15	15%	4,5	2	15	10%	3	2	15	10%	3	2	15	10%	3	2	15	5%	1,5	2	15	5%	1,5	30			100%
	EXISTENCIA DE DOCUMENTOS DE ADQUISICIÓN DE EQUIPOS Y SOFTWARE Y CONTRATOS LEGAL DE PROVEEDOR DE INTERNET Y RED (ISP).	2	15	10%	3,00	2	15	15%	4,5	2	15	10%	3	2	15	10%	3	2	15	10%	3	2	15	10%	3	2	15	10%	3	2	15	15%	4,5	2	15	5%	1,5	2	15	5%	1,5	30			100%
	DOCUMENTACIÓN DE LOS SISTEMAS UTILIZADOS PARA LOS SERVICIOS DE LA EMPRESA.	2	15	20%	6,00	2	15	10%	3	1	15	15%	2,3	1	15	15%	2,3	2	15	10%	3	1	15	5%	1	1	15	10%	2	1	15	10%	1,5	1	15	5%	0,75	2	15	0%	0	21			100%

Br. Héctor Salgado Palacios
Br. Michael Tejeda Valenzuela

Anexo 6: Evaluación total de riesgo por área funcional.

UNIDAD ADMINISTRATIVA	ACTIVIDAD	RT % 1	RIESGO DE AUDITORÍA TOTAL POR ÁREA	NIVEL DE RIESGO
Division de Tecnologías de la Información y Comunicación	ACCESO DE LOS USUARIOS A SISTEMAS, SISTEMAS OPERATIVOS Y BASES DE DATOS.	27	30	Medio
	ACCESO DE LOS USUARIOS A PROGRAMAS Y ARCHIVOS	28		
	DISPOSICIÓN DE SISTEMAS ALTERNOS EN CASO DE FALLOS.	22		
	EXISTENCIA DE SOFTWARE DE PROTECCIÓN (ANTIVIRUS, FIREWALL.)	18		
	CONTROL DE ACCESO DE LOS USUARIOS A LOS SERVICIOS DE INTERNET.	26		
	CONTROL DE ACCESOS DE LOS USUARIOS A LOS EQUIPOS.	24		
	INFORMES DE ACCESOS Y VISITAS A LAS INSTALACIONES.	31		
	INVENTARIO DE EQUIPOS Y SOFTWARE.	25		
	REVISIÓN DE LA RED (FACTOR AMBIENTAL, FÍSICO Y HUMANO)	30		
	CONTROLES PARA LA INSTALACIÓN Y USO DE DISPOSITIVOS EXTERNOS.	40		
	RESPALDO DE INFORMACIÓN CRITICA	40		
	PLAN DE CONTINUIDAD	40		
	PLAN DE CONTINGENCIA	40		
	PLAN DE MANTENIMIENTO DE HARDWARE Y SOFTWARE	40		
	DISPOSICIÓN DE MANUALES DE USUARIO Y DE INSTALACIÓN DE LOS SISTEMAS.	30		
	EXISTENCIA DE DOCUMENTOS DE ADQUISICIÓN DE EQUIPOS Y SOFTWARE Y CONTRATOS LEGAL DE PROVEEDOR DE INTERNET Y RED (ISP).	30		
	DOCUMENTACIÓN DE LOS SISTEMAS UTILIZADOS PARA LOS SERVICIOS DE LA EMPRESA.	21		

Anexo 7: Gráfico de evaluación de riesgos.



Anexo 8: Programas de auditoría.

Componente: Acceso de los usuarios a sistemas, sistemas operativos y bases de datos.

Programa de Auditoría	
Dominio	Entregar dar Servicios y Soporte (DSS)
Proceso	DSS05: Gestionar los Servicios de Seguridad.
Objetivo de Control	Verificar la implementación de controles adecuados para los accesos de los usuarios.
No.	Procedimiento
1	Solicitar listado de usuarios que tienen acceso a los sistemas usados en los equipos
2	Corroborar si existe en cada equipo una cuenta de usuario en el sistema operativo para cada persona.
3	Verificar cuantos de los usuarios tiene login y password para ingresar a sistemas de gestión de aduanas y bases de datos.

Componente: Acceso de los usuarios a programas y archivos

Programa de Auditoría	
Dominio	Entregar dar Servicios y Soporte (DSS)
Proceso	DSS06: Gestionar los Controles de los Procesos del Negocio.
Objetivo de Control	Verificar la aplicación de normas acceso de los usuarios a la modificación de archivos y manipulación de programas no propios del trabajo.
No.	Procedimiento
1	Mediante la observación identificar si los usuarios tienen acceso a la información almacenada en los equipos sin ninguna restricción.
2	Comprobar la existencia de medidas de restricción a los usuarios en el uso de archivos en las Pécs y así mismo de la manipulación y ejecución de programas ajenos al giro de la empresa.

Componente: Disposición de sistemas alternos en caso de fallos.

Programa de Auditoría	
Dominio	Entregar dar Servicios y Soporte (DSS)
Proceso	DSS04: Gestionar la Continuidad.
Objetivo de Control	Obtener un plan de contingencia (Si es que existe), en caso de que los sistemas principales fallaran.
No.	Procedimiento
1	Aplicar entrevista al encargado del área para conocer con que tipos de medidas cuentan, en caso de fallar uno de los sistemas.
2	Verificar la existencia de servidor alterno donde se almacene la información de clientes y gestiones diarias.

Componente: Existencia de software de protección (antivirus, firewall.)

Programa de Auditoría	
Dominio	Entregar dar Servicios y Soporte (DSS)
Proceso	DSS03: Gestionar los Problemas.
Objetivo de Control	Evaluar el tipo de software y licencias obtenidas, su desempeño y que sean acorde con el tipo de empresa.
No.	Procedimiento
1	Asegurar mediante la observación directa la existencia de software de protección en cada uno de los equipos.
2	Si existe el software verificar si se encuentra actualizado.

Componente: Control de acceso de los usuarios a los servicios de Internet.

Programa de Auditoría	
Dominio	Entregar dar Servicios y Soporte (DSS)

Proceso	DSS02: Gestionar las Peticiones y los Incidentes del Servicio
Objetivo de Control	Revisar la implementación de controles para el uso de Internet.
No.	Procedimiento
1	Mediante entrevista al encargado del área, se pretende conocer si en la empresa hay un reglamento de uso del servicio de Internet, para los usuarios que acceden a los equipos.
2	En caso de que existan reglas para el uso, verificar mediante la observación si dichas reglas son las correctas para el óptimo uso de dicho servicio.

Componente: Control de accesos de los usuarios a los equipos

Programa de Auditoria	
Dominio	Construir, Adquirir e Implementar (BAI)
Proceso	BAI03: Gestionar la Identificación y la Construcción de Soluciones
Objetivo de Control	Verificar los normativos de uso y acceso a los equipos.
No.	Procedimiento
1	Solicitar al encargado del área la lista de equipos que se usan, cuantos usuarios las usan y cuantas horas al día son usados estos equipos.

Componente: Informes de accesos y visitas a las instalaciones.

Programa de Auditoria	
Dominio	Entregar dar Servicios y Soporte (DSS)
Proceso	DSS01: Gestionar las Operaciones
Objetivo de Control	Revisar el control de visitas a las instalaciones de informática (si existe).
No.	Procedimiento

1	Verificación de los sistemas y mecanismos de seguridad sobre el ingreso al área de operaciones mediante el proceso de observación directa.

Componente: Inventario de equipos y software

Programa de Auditoría	
Dominio	Construir, Adquirir e Implementar (BAI)
Proceso	BAI03: Gestionar la Identificación y la Construcción de Soluciones
Objetivo de Control	Verificar si existe un inventario y corroborar la información del inventario con lo existente en la empresa.
No.	Procedimiento
1	Aplicar entrevista al encargado del área para conocer la existencia de inventario de equipos y software de respaldo en caso de que un equipo o programa falle.
2	En caso de que exista un inventario, verificar su existencia visitando el lugar de almacenamiento

Componente: Revisión de la red (Factor Ambiental, Físico y Humano)

Programa de Auditoría	
Dominio	Entregar dar Servicios y Soporte (DSS)
Proceso	DSS05: Gestionar los Servicios de Seguridad
Objetivo de Control	Examinar la red física, la disposición de los equipos involucrados en esta y los usuarios que tiene contacto directo con ella.
No.	Procedimiento
1	Revisión mediante la observación directa de la instalación de la red y los equipos para ver si esta implementada de forma correcta.

Componente: Controles para la instalación y uso de dispositivos externos.

Programa de Auditoría	
Dominio	Entregar dar Servicios y Soporte (DSS)
Proceso	DSS02: Gestionar las Peticiones y los Incidentes del Servicio
Objetivo de Control	Verificar si existe algún control para el uso de periféricos, las restricciones y su alcance.
No.	Procedimiento
1	Aplicar entrevista al encargado del área para comprobar si utilizan algún método en los equipos para restringir el acceso de dispositivos externos o bien si existe un reglamento para el uso de estos.

Componente: Respaldo de información crítica

Programa de Auditoría	
Dominio	Entregar dar Servicios y Soporte (DSS)
Proceso	DSS05: Gestionar los Servicios de Seguridad.
Objetivo de Control	Verificar si existen respaldos en digital de la información vital de clientes y procesos importantes para la empresa.
No.	Procedimiento
1	Aplicar entrevista para conocer la existencia de respaldos de la información que usan en las gestiones diarias.
2	Si existen respaldos, verificar que tipo de respaldos son (digitales o físicos), si son digitales en que se almacenan (servidor alterno, discos, memorias u otros dispositivos externos).

Componente: Plan de Continuidad

Programa de Auditoría	
Dominio	Entregar dar Servicios y Soporte (DSS)
Proceso	DSS04: Gestionar la continuidad.
Objetivo de Control	Comprobar la existencia de un plan de continuidad que se use en casos de desastre naturales o accidentes provocados por la naturaleza humana y que puedan detener totalmente las operaciones de la empresa.
No.	Procedimiento
1	Realizar entrevista a la encargada del área de mantenimiento para conocer si existe un plan de continuidad para estar listos ante un desastre natural o causado por la misma naturaleza humana y que pueda detener totalmente las operaciones.
2	Si este plan existe, solicitar detalles del mismo y de los pasos que se realizarían al momento de surgir un caso de estos que pueda detener las operaciones totales de las operaciones.

Componente: Plan de Contingencia

Programa de Auditoría	
Dominio	Entregar dar Servicios y Soporte (DSS)
Proceso	DSS04: Gestionar la continuidad.
Objetivo de Control	Determinar si el plan de contingencia es lo suficientemente específico o detallado para poder continuar con las operaciones en la empresa y que, además, dicho plan este acorde a lo que la empresa tiene en sus recursos (Si dicho plan existe).
No.	Procedimiento
1	Realizar entrevista a la encargada del área de mantenimiento, para conocer si existe un plan de contingencia al momento de un fallo.

2	Si existe el plan de contingencia, solicitar detalles de loque se hace al momento de surgir un fallo que detenga parcialmente las actividades en la empresa.

Componente: Plan de Mantenimiento de Hardware y Software

Programa de Auditoría	
Dominio	Construir, Adquirir e Implementar (BAI)
Proceso	BAI03: Gestionar la Identificación y la Construcción de Soluciones.
Objetivo de Control	Revisar el plan de mantenimiento al software, si el periodo entre cada mantenimiento es el adecuado y si se hace el mantenimiento como se debe.
No.	Procedimiento
1	Comprobar la existencia de un plan de mantenimiento mediante entrevista a la encargada del área de mantenimiento.
2	Si este plan existe, conocer qué tipo de plan se tiene, y que detalles abarca el mismo para el mantenimiento de equipos y software en general de la empresa.

Componente: Disposición de manuales de usuario y de instalación de los Sistemas

Programa de Auditoría	
Dominio	Construir, Adquirir e Implementar (BAI)
Proceso	BAI02: Gestionar la Definición de Requisitos
Objetivo de Control	Revisar los manuales de usuarios de los programas que están actualmente en uso y si estos manuales son los más actuales.
No.	Procedimiento
1	Solicitar los manuales de usuario de los sistemas que utilizan para la gestión de servicios que la empresa brinda.

2	Revisar los manuales para observar si son acordes a la versión del software que se está usando.

Componente: Existencia de documentos de adquisición de equipos y software y contratos legal de proveedor de Internet y red (ISP).

Programa de Auditoría	
Dominio	Construir, Adquirir e Implementar (BAI)
Proceso	BAI03: Gestionar la Identificación y la Construcción de Soluciones.
Objetivo de Control	Verificar las compras de equipos mediante documentos legales (facturas) y revisar el contrato de ISP (Internet servicie proveer) para determinar lo estipulado en el contrato y verificar su correcto cumplimiento.
No.	Procedimiento
1	Solicitar al encargado del área de mantenimiento el registro o respaldo de facturas donde se demuestre la adquisición de equipos, software y servicio de Internet.

Componente: Documentación de los sistemas utilizados para los servicios de la empresa.

Programa de Auditoría	
Dominio	Construir, Adquirir e Implementar (BAI)
Proceso	BAI02: Gestionar la Definición de Requisitos
Objetivo de Control	Determinar si existe la documentación de los sistemas adquiridos por la empresa y si esta posee todos los aspectos necesarios para poder dar mantenimiento al sistema en caso de ser necesario.
No.	Procedimiento
1	Mediante la técnica de la entrevista conocer si la empresa al adquirir un sistema obtiene la documentación (diagramas, arquitectura, código) de estos para poder ser modificados.