VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRIA EN EVALUACION Y AUDITORIA DE SISTEMAS

III PROMOCION

TESIS DE GRADO MAESTRIA EN EVALUACION Y AUDITORIA DE SISTEMAS

Tema: "AUDITORIA INFORMATICA BASADA EN EL ANALISÍS DE RIESGOS A LA EMPRESA TECNISEGUROS S.A."

AUTORES:

JULIO CÉSAR CALDERÓN CARRASCO

DAVID ADOLFO OCAÑA ALDAZ

DIRECTOR:

EC. GABRIEL CHIRIBOGA

SANGOLQUÍ, ABRIL 2014

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por los Ingenieros: Julio César Calderón Carrasco y David Adolfo Ocaña Aldaz como requerimiento parcial a la obtención del título de MAGISTER EN EVALUACION Y AUDITORIA DE SISTEMAS.

Sangolquí, 30 de Abril del 2014

_____

Eco. Gabriel E. Chiriboga B. MSI.

Director del Proyecto.

AUTORIA DE RESPONSABILIDAD

Ing. Julio César Calderón Carrasco

E

Ing. David Adolfo Ocaña Aldaz

DECLARAMOS QUE:

La tesis de grado titulada: "Auditoría Informática Basada en el Análisis de Riesgos de la Empresa TECNISEGUROS S.A", ha sido desarrollada con base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de nuestra autoría.

Sangolquí, 30 de Abril del 2014

Ing. Julio César Calderón Carrasco 171608387-6.	Ing. David Adolfo Ocaña Aldaz. 172043760-5

AUTORIZACIÓN

Nosotros:

Ing. Julio César Calderón Carrasco

E

Ing. David Adolfo Ocaña Aldaz

Autorizamos a la Universidad de las Fuerzas Armadas la publicación, en la biblioteca virtual de la institución del trabajo: "Auditoría Informática Basada en el Análisis de Riesgos de la Empresa TECNISEGUROS S.A", cuyo contenido, ideas, y criterios son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, 30 de Abril del 2014

Ing. Julio César Calderón Carrasco 171608387-6.	Ing. David Adolfo Ocaña Aldaz. 172043760-5

DEDICATORIA

Este trabajo lo dedicamos a nuestros padres y madres por su entrega y apoyo incondicional a lo largo de nuestros estudios. A nuestras familias que siempre nos vieron grandes y nos inspiran a continuar superándonos. A nuestras novias por sus valores de excelencia y compromiso que utilizamos a lo largo de estos estudios y por su amor incondicional. Y a Dios por permitirnos tener la oportunidad de estudiar y crecer como personas y profesionales.

Ing. Julio César Calderón Carrasco

Ing. David Adolfo Ocaña Aldaz.

AGRADECIMIENTO

Mi agradecimiento especial para:

La Universidad de las Fuerzas Armadas por habernos permitido desarrollar nuestro potencial profesional. A la empresa Tecniseguros S.A, por apoyarnos y permitirnos desarrollar el proyecto de tesis.

A nuestro director de proyecto de tesis, Eco. Gabriel Chiriboga, por su valioso aporte y conocimientos impartidos.

Ing. Julio César Calderón Carrasco

Ing. David Adolfo Ocaña Aldaz.

Contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Este proyecto tiene como objetivo analizar la situación en la que se encuentra el Departamento de Tecnologías de Información para la empresa Tecniseguros S.A. mediante el desarrollo de una Auditoría Informática Basada en el análisis de riesgos identificándolos con la metodología MAGERIT 3.0 y siguiendo los lineamientos del marco de referencia COSO ERM, el cual contempla las siguientes etapas: Ambiente de Control, Establecimiento de Objetos, Identificación de Eventos, Evaluación y Análisis de Riesgos, Respuesta al Riesgo, Actividades de Control, Información y Comunicación, Monitoreo. Tecniseguros S.A cuenta con un desarrollo interno de software, orientado a los procesos del negocio, esto ha generado un desorden en los aplicativos resultantes, con un importante número de ejecutables aislados, en este momento están desarrollados en diferentes versiones y en diferentes bases de datos, teniendo dependencia hacia los desarrolladores. Al finalizar el proyecto de auditoría Tecniseguros S.A contará con el Análisis de Riesgos de TI, Niveles de Madures de sus Procesos basándose en el Marco de referencia COBIT 4.1 y el informe de auditoría con sus respectivas Observaciones y Recomendaciones sobre acciones prioritarias a tomar.

PALABRAS CLAVE: RIESGO INFORMÁTICO, METODOLOGÍA DE ANÁLISIS DE RIESGOS, AUDITORIA INFORMÁTICA, MARCO DE REFERENCIA, NIVEL DE MADUREZ

ABSTRACT

This project aims to analyze the situation in which it is the Department of Information Technology for the company Tecniseguros SA through the development of a Computer -Based Audit Risk Analysis 3.0 MAGERIT identifying them with the methodology and following the guidelines of COSO ERM framework , which includes the following steps: Control Environment , Objects Setting , Event Identification , Evaluation and Risk Analysis , Risk Response , Control Activities , Information and Communication , Monitoring It is necessary to indicate that Tecniseguros SA to be a company that has an internal software development oriented to the main processes generates a disorder resulting in applications with a large number of isolated executable, developed in different versions in different databases having a high dependence on developers when comparing to benchmarks and best practices suggests establishing and determining risk levels and response to these drawbacks. Upon completion of the project will Tecniseguros SA Risk Analysis IT maturity levels of their processes based on COBIT Framework 4.1 and the audit report with their observations and recommendations on priority actions to take.

KEYWORDS: COMPUTER RISK, RISK ANALYSIS METHODOLOGY, AUDIT FRAMEWORK, MATURITY LEVEL

1. CAPÍTULO I

1.1. Introducción a Tecniseguros S.A.

Tecniseguros S.A. es una empresa de Grupo Futuro. Los sistemas de Tecniseguros S.A. responden a los diferentes procesos organizacionales, la parte financiera, registro de operaciones y la emisión de estados financieros.

En la página web de Tecniseguros se encuentra que, "Tecniseguros S.A. nació como una alternativa innovadora en 1973" también menciona que, desde entonces han marcado la pauta en el corretaje y asesoría de seguros en distintos niveles. (Tecniseguros, http://www.tecniseguros.com.ec/trayectoria, 2013).

1.2. Justificación e importancia

El aporte de esta auditoría informática de la Empresa Tecniseguros S.A, es servir de herramienta base, mediante la cual, se identifican los riesgos del área de tecnología, se categorizan los riesgos de acuerdo a su probabilidad e impacto, sugiere una respuesta al riesgos y termina con un informe de auditoría en el que se destacan las principales observaciones.

La Auditoría Informática basada en el Análisis de Riesgos de tecnologías de Información para nos permitirá contar con un diagnostico segregado de la situación actual y poder tomar medidas de acción, esto se realiza con la finalidad de, alienar y optimizar los recursos tecnológicos con las políticas empresariales, siguiendo los lineamientos de los marcos de referencia COSO ERM (Organizations, 2014).

Un aporte adicional de este proyecto de titulación es establecer niveles de madures a sus procesos basados en COBIT 4.1 (Association, 2013) para completar el proceso de la auditoria, agrupando y relacionando el proceso involucrado con el dominio correspondiente.

Esta investigación es de tipo Inductiva, se basara en el concepto global para llegar a lo específico. El método iniciará con la identificación de cada una de las variables de la problemática establecida, de esta manera se establecerá la relación causa - efecto

entre los elementos que componen la investigación, logrando una síntesis de la problemática.

Las técnicas y procedimientos para recolectar la información para esta investigación serán la observación y la encuesta; en observación se analiza el flujo de la información en todos los procesos, llevados a cabo por los dueños o responsables, la encuesta que se realizará a los clientes o usuarios de los sistemas, con el fin de conocer sus opiniones y observaciones.

La información obtenida es tabulada y sometida a técnicas matemáticas de tipo estadístico y manejo de porcentajes, para lo cual se elaboran tablas estadísticas cuyos valores están representados en porcentajes, a continuación se representa gráficamente esta información para proceder al análisis e interpretación de resultados

Estos resultados sirven de guía para reforzar los procesos críticos, con mayores riesgos y amenazas, así como evaluar la participación de recursos en procesos que son considerados no críticos para la empresa.

La metodología COBIT 4.1 (Association, 2013) es utilizada para determinar el nivel de madurez de cada proceso, todos estos son detallados con sus riesgos.

Esta auditoría informática basada en el análisis de riesgos beneficiara indirectamente a los usuarios de los aplicativos en virtud que se emplearan controles para garantizar que el funcionamiento no se vea afectado así como también se reducirá el tiempo de ejecución de los procesos en casos de contingencias o planes de continuidad, ya que tendrán claramente identificado los procesos críticos y riesgos de cada unidad

Tecniseguros S.A no necesita realizar adquisición de licencias o permisos para la ejecución de la presente auditoria y los gastos operativos serán asumidos por los autores del proyecto.

Los medios o recursos empleados para el proyecto son material de los autores y documentación entregada por la Universidad de las Fuerzas Armadas mediante sus catedráticos

1.3. Planteamiento del problema

El equipo de desarrollo Tecniseguros S.A está encargado de atender los requerimientos funcionales del negocio, diseñando, desarrollando e implementando sistemas y manteniendo y realizando cambios en los sistemas actuales.

El equipo trabaja con alrededor de 200 aplicaciones, entre las que podemos citar al sistema principal, mantenimiento de productos, reportería, gestión de renovaciones, cotizadores, entre otros. Estas aplicaciones se ejecutan como aplicaciones cliente servidor y aplicaciones web, con acceso a datos que se encuentran en un repositorio centralizado, constituido por varias bases de datos, distribuidas geográficamente en un motor MSQL 2008 como podemos ver en la figura 1.

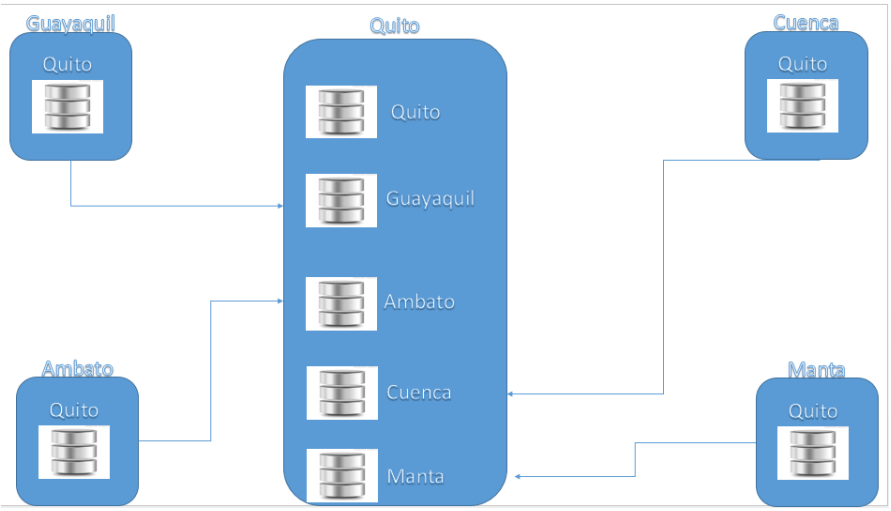


Figura 1. “Distribución Geográfica de Bases de Datos”

Las bases de datos se encuentran distribuidas geográficamente y se replican mediante con la base de datos central, no existe una base de datos única y cada localidad tiene su propia base de datos.

No existe una normativa o estándar de desarrollo, formal o informal, dificultando el desarrollo de nuevas aplicaciones o el mantenimiento de las existentes. Al existir una única base de datos, sobre la que todas las aplicaciones tienen acceso, existe el riesgo de afectar dicha base al modificar un programa.

La empresa tiene alta dependencia de los desarrolladores, debido a su conocimiento, lo que trae complicaciones cuando estas personas se encuentran

ausentes o se separan de la empresa, elevando los tiempos de respuesta o causando paralización del servicio.

El trabajo de aseguramiento de la calidad tiene toda la responsabilidad de validar las aplicaciones, no existen ambientes homogéneos de desarrollo, pruebas y control de calidad, esto genera riesgo al momento de pasar a producción las nuevas aplicaciones o sus modificaciones, y, en muchos casos únicamente se valida el impacto del cambio en la aplicación y no en todas las aplicaciones, por lo que, a veces, este control llega a fallar.

No existe un mapa de las aplicaciones y sus relaciones con la base de datos única, por lo que, no se conoce las relaciones entre todas ellas.

Las aplicaciones son validadas por el mismo desarrollador y el asegurador de calidad, pero la verificación se realiza en la misma máquina del desarrollador y las pruebas reales se hacen en producción, en donde los usuarios son quienes reportan los fallos.

Existe un alto pedido de cambios en el funcionamiento de las aplicaciones, generalmente con tiempos cortos de desarrollo y pruebas, tampoco existe conciencia sobre las actividades de estabilización de las aplicaciones.

Existen aplicativos aislados y ejecutables desarticulados que se conectan a una misma base de datos donde por ejemplo, la página principal del core es una aplicación Windows la cual llama a una página web y dependiendo el modulo seleccionado llama a otro ejecutable o sistema web independiente al que se está gestionando.

1.4. Formulación del problema a resolver

El propósito de este proyecto es Auditar a la empresa Tecniseguros S.A., específicamente al Departamento de Tecnología, enfocándose a los procesos existentes, mismos que se analizan en el capítulo 3, relacionando los activos que intervienen en cada uno de ellos para identificar sus riesgos y empleando la metodología de análisis de riesgos.

1.5. Objetivos

1.5.1. Objetivo general

Desarrollar la Auditoría Informática Basada en el Análisis Riesgos de la Empresa TECNISEGUROS S.A. empleando metodologías y marcos de referencia establecidos.

1.5.2. Objetivos específicos

- Identificar los procesos del área de TI.
- Identificar los riesgos en los todos los procesos de Ti mediante la aplicación de la metodología Magerit 3.0 (Electrónica, 2014).
- Ejecutar un análisis de riesgos de los sistemas de información de Tecniseguros S.A. utilizando el marco de referencia COSO ERM (Organizations, 2014).
- Desarrollar la matriz de riesgos.
- Determinar los niveles de madurez de los procesos de Ti utilizando el marco de referencia COBIT 4.1 (Association, 2013).
- Ejecutar los procesos de Auditoría Informática.
- Presentar el Informe de Auditoria Informática.

2. CAPÍTULO II

2.1. Antecedentes del estado del arte

Existen diferentes tipos de auditorías en esencia todas ellas mantienen los mismos fundamentos. La auditoría financiera tradicional evoluciona y genera una rama especializada, es aquí donde surge la auditoria Informática. Se publican diferentes estudios e investigaciones que dan como resultado publicaciones en todo el mundo sobre la auditoria informática, especificando procedimientos y metodologías. (Source, 2013)

La auditoría informática continua su evolución, adaptándose a los diferentes reglamentos y necesidades de las organizaciones, sin embargo, las áreas de riesgos empezaron a ver la auditoría como una herramienta para manejar sus riesgos y es como nace la auditoría basada en riesgos.

La auditoría basada en un análisis de riesgo se apoya en varias normativas, a continuación se mencionan algunas de ellas:

- IT Governance Institute ITGI
- Standards, Guidelines and Procedures for information system auditing
- Framework COBIT 5
- Val IT (Getting best value from IT investments)
- Risk IT
- Information System Control Journal
- Itil V3
- COSO ERM

El análisis de riesgos es una rama complementaria a la auditoría, está enfocada en evidenciar las vulnerabilidades y amenazas de una organización, este enfoque permite enfocar los recursos que inviernen en una auditoría y concentrarse únicamente en los puntos que presentan riesgos o mayor impacto a la organización.

El riesgo es la combinación de una vulnerabilidad y una amenaza, si una de las dos no existe, el riesgo desaparece. Las amenazas por lo general son externas, aunque las estadísticas de ataques exitosos, están cambiando este pensamiento, en la imagen

1, “The source of greatest risk to sensitive data”, se muestra que la principal fuente de amenazas son usuarios internos. (IBM, 2012)

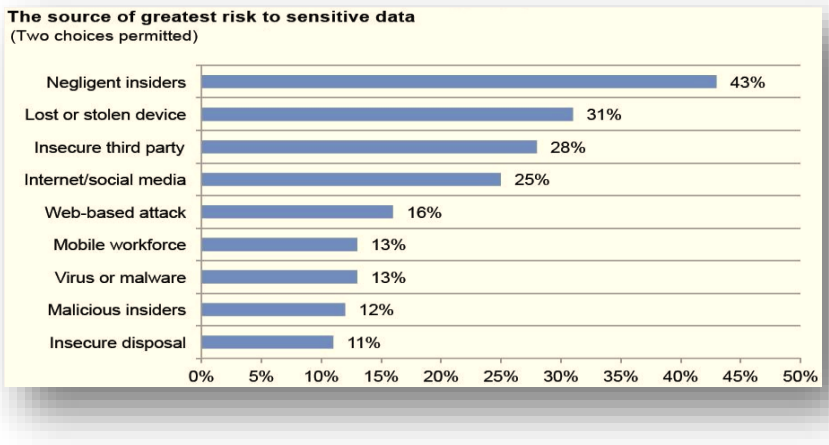


Figura 2. “The source of greatest risk to sensitive data”

La auditoría basada en riesgos permite generar nuevas estrategias para garantizar la mejor operación posible de una organización, optimizando los recursos de la auditoría y convirtiéndose en un método preventivo y proactivo.

2.2. Marco Teórico

La auditoría basada en el Análisis de riesgos que planteamos en este proyecto de titulación emplea dos metodologías, por un lado el marco de referencia COSO ERM para el manejo de riesgos y la metodología Magerit 3.0 para la identificación de Amenazas.

El objetivo de esta auditoria es de manera preventiva ante las posibles amenazas y ocurrencias en el caso de no tomar medidas de control que pueden afectar a la continuidad del negocio.

La metodología de esta auditoria se basa en tres puntos:

- Establecer las causas de los riesgos potenciales
- Determinar por qué se generan
- Evaluar el posible impacto

El resultado de este proceso es un informe de auditoría basado en riesgos para determinar las observaciones (hallazgos) y recomendaciones.

La auditoría basada en riesgos toma los marcos de referencia establecidos por (ISACA, 2010), que indica que:

"La función de auditoria debe ser gestionada y conducida en una forma que asegure que las diversas tareas realizadas y logradas por el equipo de auditoria cumplirán los objetivos de la función de auditoria, mientras se preserva la independencia y competencias de la auditoria".

Un enfoque más ampliado lo establece (Jeremías, 2011) quien determina que, la Auditoría de Gestión a las Tecnologías de Información y Comunicaciones es imparcial con respecto a:

- Eficiencia en el uso de los recursos informáticos
- Confidencial, Integral, Oportuna y Confiable de la información
- Efectividad de los controles establecidos y
- La optimización de los recursos tecnológicos

2.3. Elementos de Apoyo

2.3.1. Marco de referencia Cobit 4.1

Es una guía de las mejores prácticas dirigida al control y supervisión de tecnología de la información con varios recursos enfocados en tener un buen gobierno corporativo que apoye a la búsqueda de satisfacer la necesidad de asegurar el valor en la manejo de las tecnologías de información, donde según la aplicación de las mejores prácticas otorga valores de cumplimiento o madurez de los dominios; partiendo de 0 (cero) cuando las practicas sugeridas son inexistentes hasta llegar al máximo nivel de 5 (cinco) cuando estas se encuentran implementadas, funcionales y optimizadas en su totalidad.

La evaluación de los niveles de madurez de los dominios de COBIT se los determinara relacionándolos con los procesos existentes en el área de TI.

Las necesidades empresariales están enfocas hacia los dominios de:

- Planear y Organizar (PO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Además la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente se debe implementar una estructura Organizacional y una estructura tecnológica apropiada

- Adquirir e Implementar (AI)

Para llevar a cabo la estrategia de TI, las soluciones que TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Además el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio

- Entregar y Dar Soporte (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, los que incluyen la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativas.

En la figura 3, cubo de COBIT 4.1, se muestran los dominios:

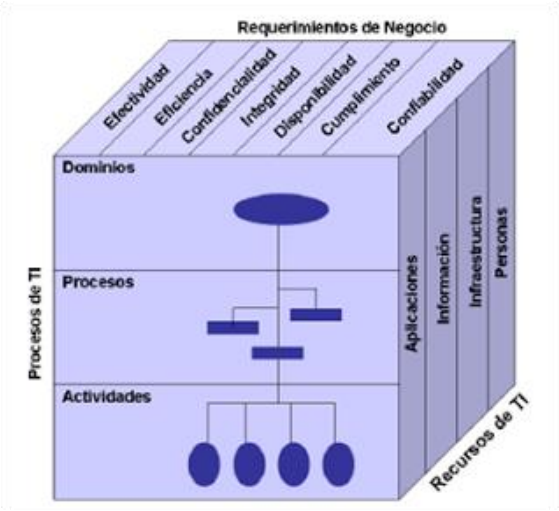


Figura 3. “Cubo de COBIT 4.1”

Modelo de madurez.

El modelo de madurez de Cobit permite identificar el nivel de cumplimiento de los procesos de TI, una vez que han sido evaluados durante la ejecución de la auditoría informática. Para calcular el rango del nivel de madurez de los procesos de TI se realizó la división del cien por ciento para los seis niveles de madurez. El modelo de madurez se clasifica de acuerdo a la tabla 1, Modelo de madurez.

Tabla 1
Modelo de madurez

NIVEL	DESCRIPCIÓN
0	No existente
1	Inicial
2	Repetible
3	Definido
4	Administrado
5	Optimizado

2.3.2. Metodología Magerit para el análisis de riesgos

Magerit ofrece un método sistemático para analizar riesgos y ayudar a descubrir y planificar las medidas oportunas para mantenerlos bajo control. Además realiza procesos de evaluación, auditoría, certificación y acreditación, según corresponda.

También se ha buscado la uniformidad de los informes que recogen los hallazgos y las conclusiones de un proyecto de análisis y gestión de riesgos: Modelo de valor caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos. Mapa de riesgos Relación de las amenazas a que están expuestos los activos. Evaluación de salvaguardas Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan. Estado de riesgo Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas. Informe de insuficiencias Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema. Plan de seguridad Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos.

Teniendo en cuenta las diferentes dimensiones de la seguridad: Disponibilidad: o disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones. Integridad: o mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización. Confidencialidad: o que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autoriza- dos. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos. Autenticidad (de quién hace uso de los datos o servicios): o que no haya duda de quién se hace responsable de una información o prestación de un servicio, tanto a fin de confiar en él como de poder perseguir posteriormente los incumplimientos o errores.

El uso de esta metodología será enfocado en detallar según los procesos de la compañía el listado de activos que intervienen o se ven afectados en cada proceso para finalmente poder obtener los riesgos que afectan a los activos y en consecuencia los riesgos por procesos siendo este nuestro punto de partida para proceder a tratar y analizar el riesgo con el Marco de referencia COSO.

Los procesos que se analizan son:

- Adquisiciones Garantías Equipo Electrónico (P11-01)
- Soporte Técnico (P11-02)
- Administración de Respaldos (P11-03)
- Administración Data Center (P11-04)
- Administración Redes LAN (P11-05)
- Administración Redes WAN (P11-06)
- Mantenimiento de Hardware (P11-07)
- Mantenimiento De Licencias (P11-08)
- Desarrollo y Mantenimiento de Aplicaciones (P11-09)
- Administración de Servidores (P11-10)
- Administración de usuarios (P11-11)

En el Anexo 2 en la página 88 se detallan los activos identificados en cada uno de los 11 procesos, mismos que son utilizados en el punto de identificación de eventos.

2.3.3. Marco de referencia COSO ERM

El marco de referencia COSO ERM se utiliza para el análisis de riesgos.

Hace más de una década el Committee of Sponsoring Organizations of the Treadway Commission, conocido como COSO, publicó el Internal Control Integrated Framework para facilitar a las empresas a evaluar y mejorar sus sistemas de control interno. Desde entonces ésta metodología se incorporó en las políticas, reglas y regulaciones y ha sido utilizada por muchas compañías para mejorar sus actividades de control hacia el logro de sus objetivos. (Guerra, 2013)

Las tereas que se realizaran en los dominios de COSO ERM se muestran en la figura 4, Cubo de COSO ERM.

Figura 4: “Cubo de COSO ERM”

Esta auditoría utiliza los 8 dominios pero está orientado a una unidad de negocio, Tecnologías de Información. Aquí se numeran los 8 dominios que son cubiertos con la normativa:

- Ambiente de control
- Establecimiento de objetivos
- Identificación de eventos
- Evaluación de riesgos
- Respuesta al riego
- Actividades de control
- Información y comunicación
- Monitoreo

El marco de referencia COSO ERM plantea preguntas en cada uno de sus dominios, el detalle de estas se describen en el anexo 1 en la página 85. COSO ERM.

Los datos del análisis se recogen en una hoja de cálculo. Misma que es parte del anexo 3 en la página 97.

2.3.3.1. Escala de Evaluación de Impacto

El impacto es un valor calculado, es el resultado de multiplicar la probabilidad por el impacto. Estos valores son utilizados específicamente para el análisis de los procesos de tecnología. El resultado se clasifica en 5 niveles.

Tabla 2

Evaluación de Impacto

IMPACTO	
5	Alto
4	Crítico
3	Requiere Atención
2	Manejable
1	Nulo (Sin Riesgos)

2.3.3.2. Escala de Evaluación de Probabilidad

La probabilidad de ocurrencia de un evento se clasifica a una escala basada en la experiencia del negocio, identificamos 4 niveles.

Tabla 3

Evaluación de Probabilidad

Probabilidad	
1	Baja
2	Media Baja
3	Media Alta
4	Alta

2.3.3.3. Evaluación de riesgos

El riesgo es un valor resultante, al igual que el impacto, éste es el producto de la probabilidad y el impacto, la diferencia radica en que, está orientado a los dominios de COSO ERM en lugar de a los 11 procesos de tecnología. Este punto permite clasificar al riesgo en diferentes cuadrantes.

Tabla 4

Niveles de Riesgo

Evaluación de Riesgos	
12 - 20	Alta probabilidad de impacto con alto impacto
4 - 11	Mediana probabilidad de impacto con mediano impacto
1 - 3	Poca probabilidad de impacto con poco impacto

Una vez identificado el porcentaje de ocurrencia de un riesgo, medimos el impacto, y lo colocamos en un cuadrante, como se ve en la tabla de medidas de riesgo.

Tabla 5

Medidas de Riesgo

Impacto				
5	5	10	15	20
4	4	8	12	16
3	3	6	9	12
2	2	4	6	8
1	1	2	3	4
0	1	2	3	4
	Probabilidad			

Los riesgos en color Verde, son aceptados y no tienen una respuesta mayor, salvo un caso excepcional. Son considerados pequeños y agregar controles en estos podría representar una inversión innecesaria.

Los riesgos en color naranja son tratados, los del cuadrante superior son compartidos, es decir, aunque el impacto es alto la probabilidad es pequeña por lo que no es recomendable poner controles, pero seguros y pólizas pueden constituirse en elementos requeridos. Por otro lado, los del cuadrante inferior son mitigados, es decir, la solución es aplicar controles que prevengan la ocurrencia, por ejemplo, colocar un control de accesos.

Los riesgos del color rojo son evitados, salvo excepciones, es decir, son acciones que no deben ejecutarse dentro de la empresa.

2.3.3.4. Respuesta al riesgo

La evaluación al riesgo comprende una serie de cuestionarios, enfocados en los eventos identificados, aquí se buscan los controles necesarios para combatir el riesgo. La respuesta se da en función a la probabilidad y al impacto, de acuerdo a la siguiente tabla.

Tabla 6

Medidas de la Matriz de Riesgo

Probabilidad/Consecuencia	Insignificantes	Moderado Bajo	Moderado Medio	Alto
Probable Posible Alta	Compartir: Cuando la probabilidad es baja y el impacto es alto		Evitar: En el caso que la probabilidad y el impacto son altos.	
Posible Moderada Raro	Aceptar: En el caso que la probabilidad y el impacto es bajo.		Mitigar: Cuando la probabilidad es alta y el impacto es bajo.	

Los datos evaluados se ponen en una matriz general, a modo de resumen, misma que se denomina LA MATRIZ DE RIESGOS, misma que se utiliza en el capítulo 5 en la página 38, desarrollo del proceso de auditoría.

2.4. Marco conceptual

Para el desarrollo del proyecto se utilizaran varias normativas, estándares y términos los cuales se encuentran detallados a continuación con una breve descripción.

2.4.1. Sistemas de Información (SI)

Cuando nos referimos a un SI se está haciendo referencia a toda la visión global de los recursos de información, definiendo su alcance y asegurando su integración con los otros sistemas de Información clarificando la relación que existe entre las aplicaciones y las necesidades de información de las áreas funcionales para un fin común.

2.4.2. Sistemas en Producción

Un sistema en producción es aquel que se encuentra en funcionamiento operativo dentro de la empresa, es decir es el aplicativo que en este momento se encuentran utilizando, la versión que se publicó es el producto final de todo el proceso de desarrollo.

2.4.3. Auditoria Informática

Es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, de toda Organización la Información, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas

2.4.4. Riesgo Informático

Es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo

2.4.5. Riesgo Inherente

Son los que se generan por las características propias del sujeto de la acción de control, es decir, personas, organizaciones, instituciones, etc. por la naturaleza de las actividades, funciones o programas que desarrolla.

2.4.6. Riesgo de Control

Son los que se generan por la estructura, procedimientos y diseño del Sistema de Control Interno del sujeto de la acción de control.

2.4.7. Riesgo Detección

Está relacionado con que los auditores no logren detectar los errores existentes con los Programas de trabajo diseñados y la aplicación del juicio profesional adecuado.

2.4.8. FODA

La sigla FODA, es un acróstico de Fortalezas (factores críticos positivos con los que se cuenta), Oportunidades, (aspectos positivos que podemos aprovechar utilizando nuestras fortalezas), Debilidades, (factores críticos negativos que se deben eliminar o reducir) y Amenazas, (aspectos negativos externos que podrían obstaculizar el logro de nuestros objetivos). (Matriz FODA, 2013)

2.4.9. Portafolio de proyectos

Es un proceso administrativo designado a ayudar a un organización a adquirir y ver información acerca de todos sus proyectos y programas, luego priorizar cada proyecto de acuerdo a ciertos criterios tales como valor estratégico, impacto en recursos, costos etc.

2.4.10. Riesgo

Se lo puede definir como la volatilidad o dispersión de los resultados esperados, en base a los movimientos de las variables financieras y operacionales". (Brito, 2009)

2.4.11. Clasificación del Riesgo

Los riesgos que puede enfrentar una institución financiera son: [Clasificación Del Riesgo Financiero Basado en Modelos De Calificación Difusos]

2.4.12. Riesgo Tecnológico

El riesgo tecnológico tiene su origen en el continuo incremento de herramientas y aplicaciones tecnológicas que no cuentan con una gestión adecuada de seguridad. Su incursión en las organizaciones se debe a que la tecnología está siendo fin y medio de ataques debido a vulnerabilidades existentes por medidas de protección inapropiadas y por su constante cambio, factores que hacen cada vez más difícil mantener actualizadas esas medidas de seguridad. (Revista Seguridad, 2009)

2.4.13. Control Interno

SAC (Sistema de Auditoría y Control) define a un sistema de control interno como: "un conjunto de procesos, funciones, actividades, subsistemas, y gente que son agrupados o conscientemente segregados para asegurar el logro efectivo de los objetivos y metas. (Net Consul.com, 2012)

2.4.14. Ambiente de Control

Componente que se relaciona con la cultura organizacional de la entidad, estableciendo la alta dirección normas de conducta adecuadas bajo principios éticos y honestos que sean adoptados por los miembros de la organización y sus actividades sean desarrolladas bajos ciertos principios. (Universidad de la República de Uruguay, Control Interno, 2012)

2.4.15. Evaluación de Riesgos

Concientización de las entidades financieras que existen riesgos internos y externos a los cuales están expuestos, debiendo identificar y evaluar cuáles podrían ser las causas y sus potenciales eventos, comparándolos con los objetivos de la organización. (Alfaro, 2008)

2.4.16. Actividades de Control

Delimita las políticas y procedimientos de control para minimizar la ocurrencia y el posible impacto de los riesgos identificados. (Brito, 2009)

2.4.17. Información y comunicación

La Alta dirección garantiza que existe una adecuada comunicación de las directrices políticas y procedimientos a nivel de toda la organización de tal manera que sea conocida por los miembros, la información debe estar disponible para correcta operación de sus actividades. (Brito, 2009)

2.4.18. Monitoreo

Seguimiento de la aplicación de las políticas de control interno en cada una de las áreas de la organización, de tal forma, que se pueda encontrar confiabilidad y oportunidad de las deficiencias existentes para tomar acciones correctivas e inmediatas. (Dirección y Coordinación Técnica de Planificación, 2011)

2.4.19. COSO ERM o COSO II

Committee of Sponsoring Organizations of the Treadway Commission, enuncio um marco de control mejorado del COSO, denominado COSO –ERM, (Enterprise Risk Management), basado en el riesgo. (Net Consul.com, 2012)

2.4.20. Estabelecimiento de Objetivos

La alta dirección define los objetivos de la organización y defina los potenciales eventos que pudieran ser evitados bajo ciertos parámetros formales de análisis. (Coso, 2004)

2.4.21. Identificación de Eventos

La Alta Dirección debe realizar un análisis de cuáles son los eventos o acontecimientos internos y externos que afectan a la organización, tanto a nivel interno y externo, de tal forma, que se los puede catalogar como oportunidades o riesgos. (Monografias.com)

2.4.22. Evaluación de Riesgos

Establece que los riesgos deben ser analizados en forma detallada determinado cuales son las causas que pudieran provocarlo y el nivel de impacto para la organización. (COSO ERM, 2004)

2.4.23. Respuesta al Riesgo

Determina qué va hacer con riesgos a los cuales está expuesta la organización, que puede evitar, aceptar, reducir o compartir los riesgos. (Net Consul.com, 2012)

2.4.24. Actividad de Control

Se determina las políticas, procesos, y procedimientos encaminados a tomar las acciones de respuesta al riesgo que anteriormente fueron analizados y establecidos. (Brito, 2009)

2.4.25. Supervisión

Establecer los mecanismos apropiados para determinar si los componentes anteriores se están cumpliendo cabalmente para que se puedan tomar las acciones correspondientes y necesarias. (Brito, 2009)

3. Capítulo III

El capítulo 3 inicia la evaluación de riesgos del área de TI, utiliza el modelo COSO y genera resultados en cada evaluación. Los puntos utilizados en este capítulo son:

- Ambiente de control
- Establecimiento de objetivos
- Identificación de eventos

La identificación de eventos es apoyada por la metodología MAGERIT 3.0 y se evalúan 11 procesos, mismos que se detallaron en el capítulo 2, página 6.

Los resultados del análisis se encuentran en el anexo 4 en la página 101.

3.1. Estructura Actual

3.1.1. La organización

Tecniseguros cuenta con 280 empleados de los cuales 175 trabajan en la Regional de Quito bajo la dirección de la Gerencia Regional

Tecniseguros creció bajo el ejemplo de disciplina de sus fundadores y directores, quienes han generado un ambiente de negocios ético y constructivo a lo largo del tiempo. Este progreso no sería posible sin la razón de ser de Tecniseguros que son sus clientes, muchos de los cuales le acompañan por más de 30 años con su fidelidad.

A partir de Tecniseguros nació el Grupo Futuro, manteniendo un crecimiento económico sostenible, generando fuentes de trabajo e invirtiendo en el país con capital nacional.

El Grupo Futuro está conformado por: Tecniseguros S.A., el mayor corredor de seguros del país; Seguros Equinoccial, empresa líder en seguros patrimoniales; Salud S.A. pionera en el ámbito de la medicina prepagada; Equivida S.A., la primera compañía de seguros de vida y Metropolitan Touring que con más de 50 años de trayectoria es la más importante empresa de turismo del país.

Estas empresas han sido catalogadas de acuerdo a Price Waterhouse Coopers y Revista Líderes de El Comercio, Ecuador; como las más respetadas en sus áreas de negocio.

3.1.2. Área de tecnología de información

El departamento de tecnología está considerado una fortaleza y elemento de apoyo la organización siendo el responsable del manejo de la información y aplicaciones necesarias el trabajo con los clientes, siendo una característica diferenciadora el desarrollo interno de aplicaciones,

El Departamento de Tecnología cuenta con el siguiente organigrama:

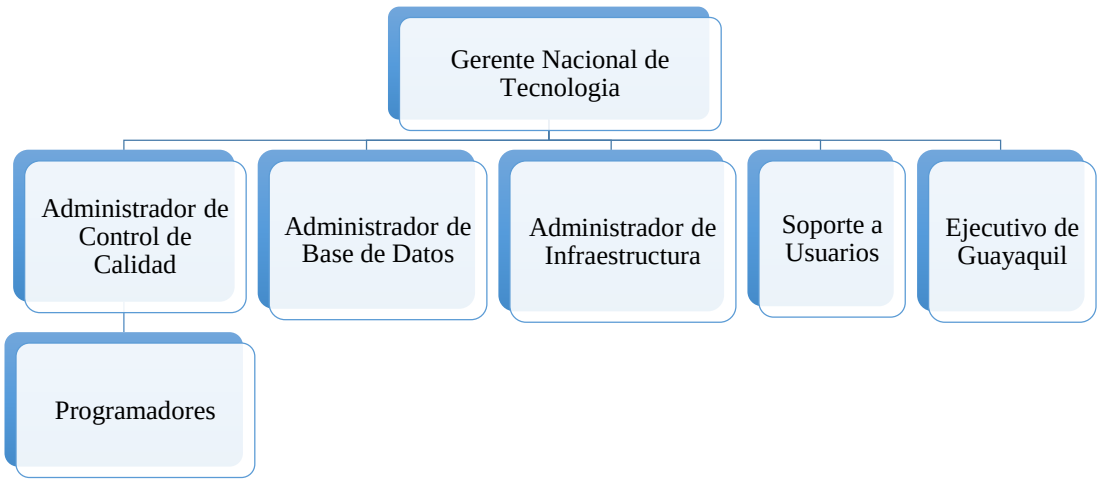


Figura 5. “Organigrama de Tecnología”

Gerente de Tecnología: Ejecutivo CIO de la empresa a cargo de los y temas de gobierno con participación en el comité ejecutivo

Atención a Usuarios: Ejecutivo responsable del soporte a los usuarios siendo el primer filtro ante fallas y errores reportados.

Administrador de Infraestructura: Ejecutivo Responsable de la Administración de los servidores, redes, respaldos y servicio de correo.

Administrador de Base de Datos: Ejecutivo responsable del monitoreo de las réplicas de las bases de datos a nivel nacional, así como la administración y mantenimiento de la misma, verificando la integridad y estándar en la nomenclatura.

Ejecutivo de Apoyo GYE: Ejecutivo responsable del soporte a los usuarios siendo el primer filtro ante fallas y errores reportados, apoyando en el área de desarrollo para aplicaciones contables.

Administrador Control de Calidad: Ejecutivo Responsable del Análisis, Diseño y coordinación del desarrollo de las aplicaciones supervisando el desarrollo de los programadores, así como también responsable del versiona miento de las fuentes y puesta en producción de los aplicativos a nivel nacional

Programador: Ejecutivo responsable del desarrollo de aplicaciones Windows y Web según los requerimientos asignados realizando la documentación técnica y manual de usuario.

A continuación se muestran los resultados del análisis, el detalle de los mismos se encuentran en el Anexo 4 en la página 101, de acuerdo al detalle de la siguiente tabla:

Tabla 7

Detalle del Anexo 4

3.2. Ambiente de control

El Entorno de Control, marca las pautas de comportamiento en una Organización y por lo tanto mantiene una influencia directa en el nivel de percepción del personal respecto al mismo, aquí se muestra el análisis de riesgos.

Los resultados muestran que existe una probabilidad del 59.11 % que ocurra una incidencia.

3.3. Planteamiento de objetivos

El análisis de este punto está orientado a descubrir cuan alineados están los objetivos de la organización con una correcta administración de riesgos con su detalle en el siguiente análisis, existe una probabilidad del 27,08 % que ocurra una incidencia, los objetivos de la organización no están orientados al manejo de riesgos, están desarrollados en función del negocio, sin embargo, son claros, están socializados, y se

evidencia el compromiso de Tecniseguros para darlos a conocer a todos los trabajadores.

3.4. Identificación de eventos

La identificación de eventos se realiza utilizando un enfoque basado en procesos. Tecniseguros S.A. tiene 11 procesos definidos, documentados, socializados y en producción en el área de Tecnología de Información.

3.4.1. Adquisiciones y Garantías Equipo Electrónico

Este proceso es el encargado según los requerimientos y necesidades de equipos realizar la respectiva cotización, compras y además realizar los trámites como coordinar garantías con el proveedor, existe una probabilidad del 12,16% que ocurra una incidencia

3.4.2. Soporte técnico

Este proceso es el encargado de Brindar soluciones a los usuarios a problemas informáticos, que permitan el desarrollo eficiente de sus actividades, existe una probabilidad del 50.00 % que ocurra una incidencia

3.4.3. Administración de respaldos

Este proceso es el encargado de salvaguardar la información de sistemas de Tecniseguros que permita el desenvolvimiento normal de las actividades en caso de problemas y contingencias, existe una probabilidad del 24.43 % que ocurra una incidencia

3.4.4. Administración del Data Center

Este proceso es el encargado de Mantener en buen estado los equipos de climatización, sistema de respaldo ininterrumpido (ups) y sistema contra incendios, y todos activos relacionados al proceso, existe una probabilidad del 43.75 % que ocurra una incidencia

3.4.5. Administración de redes LAN

Este proceso es el encargado de Velar por el correcto funcionamiento de las comunicaciones internas de cada sucursal, para el desarrollo eficiente de las actividades de Tecniseguros, existe una probabilidad del 33,72% que ocurra una incidencia

3.4.6. Administración de redes WAN

Este proceso es el encargado de Velar por el correcto funcionamiento de las comunicaciones externas, acceso a internet y enlaces entre la matriz (uio) y sus sucursales, para el desarrollo eficiente de las actividades de Tecniseguros, existe una probabilidad del 33,72% que ocurra una incidencia

3.4.7. Mantenimiento de Hardware

Este proceso es el encargado de Mantener en buen estado los equipos de sistemas utilizados en las labores de Tecniseguros, existe una probabilidad del 34.48 % que ocurra una incidencia

3.4.8. Control de Licencias

Este proceso es el encargado de Administrar las licencias adquiridas por la compañía para el desarrollo de las funciones de los ejecutivos evitando de esta manera el incumplimiento de la Ley de Propiedad Intelectual, existe una probabilidad del 34.28 % que ocurra una incidencia

3.4.9. Desarrollo y mantenimiento de aplicaciones

Este proceso es el encargado de Realizar mejoras en las aplicaciones existentes de acuerdo a los requerimientos del proceso

3.4.10. Administración de servidores

Este proceso es el encargado de Definir las pautas generales para asegurar una adecuada y efectiva realización de los procedimientos de procesamiento ya sean manuales o automáticos, que garanticen el normal funcionamiento de las operaciones de la compañía, existe una probabilidad del 43.75 % que ocurra una incidencia

3.4.11. Administración de usuarios

Este proceso es el encargado de Definir las pautas que permitan asegurar que todos los usuarios tienen exclusivamente el acceso necesario a la información para el desarrollo de sus tareas habituales en la compañía, existe una probabilidad del 50.94 % que ocurra una incidencia

Todas las evaluaciones realizadas en este capítulo generan resultados, mismos que permiten crear una respuesta a los riesgos identificados en cada proceso, el detalle de estos riesgos se encuentran en el anexo 4 en la página 101.

4. Capítulo IV

En este capítulo se realiza el análisis de los riesgos encontrados en el capítulo 3, se los analiza en base al proceso en donde se los identificó, se mide su impacto, su probabilidad y se lo coloca en un diagrama. Una vez identificados podemos definir el tratamiento que se le da, es decir, aceptar, compartir, mitigar o evitar. La respuesta al riesgo se analiza de la misma manera, enfocada en los procesos de la organización y se finaliza con la matriz de riesgos general.

A continuación se muestran los resultados del análisis, el detalle de los mismos se encuentran en el Anexo 5 en la página 140, de acuerdo al detalle de la siguiente tabla:

Tabla 8

Detalle del Anexo 5

Continua

4.1. Evaluación de riesgos

La evaluación de riesgos parte de los identificados en el capítulo anterior, mismo que se detallan en el anexo 4 en la página 101. Estos riesgos son evaluados en base a la probabilidad e impacto en la organización, la escala es definida por el personal

experto de Tecniseguros S.A, los resultados del análisis se muestran en el anexo 5 página 140

4.1.1. Mapa de Referencia al Riesgo del proceso P11-01, Adquisiciones, Garantía de equipo electrónico

La empresa tiene 45% de posibilidades que ocurra un incidente, el mismo que puede afectar al funcionamiento del negocio en un 73 %

4.1.2. Mapa de Riesgos del Proceso P11-02, Soporte Técnico.

La empresa cuenta con un nivel de 54% de posibilidades que ocurra un incidente el mismo que puede afectar al funcionamiento del negocio en un 59 %

4.1.3. Mapa de Riesgos del Proceso P11-03, Administración de Respaldos.

La empresa cuenta con un nivel de confianza del 52 %, es decir se tiene un 48% de posibilidades que ocurra un incidente el mismo que puede afectar al funcionamiento del negocio en un 80 %

4.1.4. Mapa de Riesgos del Proceso P11-04, Administración del Data Center.

La empresa cuenta con un 57% de posibilidades que ocurra un incidente el mismo que puede afectar al funcionamiento del negocio en un 59 %

4.1.5. Mapa de Riesgos del Proceso P11-05, Administración de redes LAN.

La empresa cuenta con un nivel de confianza del 50 %, es decir se tiene un 50% de posibilidades que ocurra un incidente el mismo que puede afectar al funcionamiento del negocio en un 71 %

4.1.6. Mapa de Riesgos del Proceso P11-06, Administración de redes WAN.

La empresa cuenta con un 60% de posibilidades que ocurra un incidente el mismo que puede afectar al funcionamiento del negocio en un 76 %

4.1.7. Mapa de Riesgos del Proceso P11-07, Mantenimiento de Hardware.

La empresa cuenta con un nivel de confianza del 50 %, es decir se tiene un 50% de posibilidades que ocurra un incidente el mismo que puede afectar al funcionamiento del negocio en un 72 %

4.1.8. Mapa de Riesgos del Proceso P11-08, Mantenimiento de Licencias.

La empresa cuenta con un 62% de posibilidades que ocurra un incidente el mismo que puede afectar al funcionamiento del negocio en un 57 %

4.1.9. Mapa de Riesgos del Proceso P11-09, Desarrollo y Mantenimiento de software.

La empresa cuenta con un nivel de confianza del 36,56 %, es decir se tiene un 63,44% de posibilidades que ocurra un incidente el mismo que puede afectar al funcionamiento del negocio en un 78,44 %

4.1.10. Mapa de Riesgos del Proceso P11-010, Administración de Servidores.

La empresa cuenta con un 56% de posibilidades que ocurra un incidente el mismo que puede afectar al funcionamiento del negocio en un 64 %

4.1.11. Mapa de Riesgos del Proceso P11-011, Administración de usuarios.

La empresa cuenta con un nivel de confianza del 40 %, es decir se tiene un 60% de posibilidades que ocurra un incidente el mismo que puede afectar al funcionamiento del negocio en un 83 %

4.2. Respuesta a los riesgos

Las respuestas a los riesgos están basados en los eventos identificados en la sección anterior, el detalle de la respuesta a los riesgos se encuentra en el anexo 5.

A continuación se muestran los resultados del análisis, el detalle de los mismos se encuentran en el Anexo 6 páginas 177 de acuerdo al detalle de la siguiente tabla:

Tabla 9

Detalle del Anexo 6

4.3. Actividades de control

Las actividades de control están orientadas a las recomendaciones que se van a dictar para remediar los riesgos identificados en la sección anterior.

4.4. Información y Comunicación

Este punto permite conocer las actividades de comunicación que se efectúan durante la implementación de las actividades de control.

4.5. Supervisión y monitoreo

Este punto permite dar seguimiento a las actividades de información y comunicación, mediante el monitoreo.

4.6. Mapa de riesgos generales

El presente análisis está enfocado en el manejo de los riesgos de la organización, adentrándose en el área de tecnologías de información, a diferencia del análisis de procesos anterior, este se enfoca en el manejo de riesgos generales.

El detalle de la evaluación se encuentra en el anexo 6 página 177.

4.7. Tabla general de riesgos

Esta tabla muestra el resultado de la evaluación individual de cada dominio de COSO, el detalle de la evaluación individual está en el Anexo 6 pagina 177.

El análisis de los riesgos en cada dominio de COSO permite tener los resultados de riesgo de manera individual, misma que se muestra en la tabla 10.

Tabla 10

Tabla general de riesgos

ELEMENTOS		FACORES DE EVALUACIÓN	CALIFICACIÓN POR FACTOR	CALIFICACIÓN	RIESGO DE CONTROL
1	**Ambiente Interno**	Filosofía de gestión de Riesgos	6	74/181	59,12%
		Cultura de Riesgo	15		
		Dirección	7		
		Integridad y Valores éticos	4		
		Compromiso	10		
		Estructura Organizativa	5		

Continua

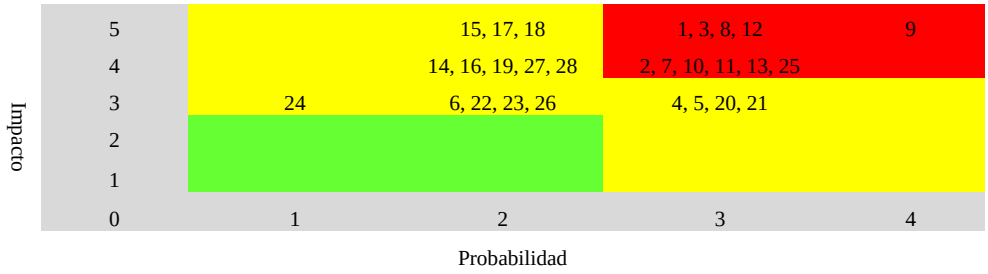
		Asignación de Responsabilidad	16		
		Políticas y Prácticas en materia de Recursos Humanos	11		
2	**Establecimiento de Objetivos**	Objetivos Estratégicos	14	36/48	25,00%
		Objetivos Relacionados	22		
3	**Identificación de Acontecimientos**	Metodologías aplicadas	10	80,2 / 130	38,31%
		Procesos	114,3		
4	**Evaluación de Riesgos**	Fuentes de datos	12	71,8/95,6	24,90%
		Procesos	59,8		
5	**Respuesta a los Riesgos**	Evaluación de Posibles Respuestas	4	12/61,0	80,33%
		Selección de Respuestas	8		
6	**Actividades de Control**	Actividades de Control (preventivas y el accionar)	23	129/238	45,80%
		Políticas y Procedimientos	30		
		Controles generales y específicos	12		
		Controles de los sistemas de información	52		
		Controles de Aplicación	12		
7	**Información y Comunicación**	Información de Riesgos	28	63/114	44,74%
		Comunicación de Riesgos	35		
8	**Supervisión**	Actividades permanentes de supervisión	18	28/64	56,25%
		Evaluación de Deficiencias	3		
		Plan de Acción	7		

4.8. Clasificación de riesgos

Los riesgos tienen un valor individual, y se los ubica en los cuadrantes que muestran la respuesta al riesgo. En la tabla 11 se muestra el número de riesgo identificado y su reacción.

Tabla 11

Clasificación de riesgos



4.8.1. Descripción de los riesgos

1. No existen políticas para manejar los riesgos a presentarse, por parte de la gerencia no se han emitido documentos formales que indiquen como proceder

2. Tecniseguros no cuenta con una política de manejo de riegos para el área de TI.

3. El personal de Tecniseguros no tiene conocimiento sobre los riesgos existentes en su trabajo, ya que los riesgos son generales pero no específicos.

4. No se ha podido evidenciar que exista documento alguno que norme los procesos de reclutamiento, creación de cuentas, roles y privilegios de personal, para ninguna de las unidades administrativas de Tecniseguros. Ni aun para el área de TIC´s.

5. No se entregan documentos donde se indique las funcionalidades que tienen los empleados dentro de la empresa

6. Si la institución posee objetivos estratégicos, pero no se encuentran alineados a los objetivos de negocio

7. No existen parámetros de medición de riesgos dentro de la empresa

8. No existe control para el Mantenimiento y desarrollo de software

9. No se identifican equipos de red perimetral orientados a la función de IPS, es decir, no existen equipos de prevención de intrusiones. La única profesión es la de un firewall y el filtrado que brinda el canal de los proveedores.

10. Existe un ecosistema de diferentes soluciones, desarrolladas a medida, con diferentes bases de datos, y sin un control de crecimiento. Existen adaptaciones de las aplicaciones que responden a la cotidianidad y no al plan estratégico de la organización o planes de Tecniseguros S.A. Las aplicaciones están desarticuladas, no integradas y cada una sirve para un propósito específico. No existe un estándar en las herramientas de desarrollo utilizadas ni en las bases de datos. Existe mucho trabajo de operación y desarrollo en el área de tecnología, tampoco existe un repositorio centralizado de código fuente y ejecutables liberados.

11. Los pases a producción no se realizan con las pruebas necesarias. Las mismas personas de desarrollo realizan las pruebas de calidad. Existe embotellamiento en la persona de control de calidad por la cantidad de pases a producción. No existe un repositorio centralizado de las versiones de los programas.

12. No existe dentro de la empresa normativas que evalúen los riesgos, la gerencia no maneja métricas para mitigar los riesgos

13. No se tiene identificado los riesgos que pudieran afectar al Área de TI de motivo por el cual es imposible poder desarrollar un plan de mitigación del riesgo ya que al no conocer con exactitud cualquier plan de respuesta estaría erróneo

14. El personal de Tecniseguros no tiene conciencia de los riesgos que pueden afectar el normal funcionamiento de la organización, de igual forma al no existir planes de respuesta al riesgo los mismos no están capacitados para la ejecución de cualquier acción en caso de alguna contingencia

15. La empresa no tiene una adecuada conciencia del riesgo, no se tiene definido cuál es la tolerancia al riesgo, ni el riesgo inherente pero aun el de control, esto puede

generar desconfianza a nivel de los clientes de la Cooperativa e inestabilidad dentro del mercado

16. No existe evidencia de haber realizado un ataque controlado a la infraestructura de Tecniseguros, o un Ethical hacking en busca de vulnerabilidades. Esto podría generar el robo o alteración de información confidencial, bloqueo de los servicios y demás inconvenientes que pueden generar graves consecuencias

17. No existen mecanismos de control de robo o adulteración de la información de los usuarios y clientes.

18. No existe evidencia de la existencia de políticas y procedimientos para el Mantenimiento y desarrollo de sistemas en el área de TI de ninguna índole

19. Las bitácoras de los sistemas, logs, flujos de red, y demás evidencia que arrojan los sistemas no se concentran en un repositorio único, haciendo que las aplicaciones dependan de especialistas para la interpretación de errores o eventos anormales. No es posible garantizar el análisis forense en base a las bitácoras en caso de ocurrir. No existe personal designado a revisar las bitácoras de los sistemas únicamente se revisan las bitácoras cuando existen inconvenientes.

20. La asignación de privilegios está relacionada a perfiles de usuario y no a las identidades de cada persona. Los privilegios se asignan individualmente en cada aplicación, la tarea está a cargo, generalmente, del administrador del sistema. No se observan actividades de conciliación y reconciliación de usuarios en las aplicaciones y recursos informáticos.

21. No se encuentran controles que permitan conocer el uso o abuso de las cuentas privilegiadas de los sistemas, tales como root, admin, etc.

22. El personal de tecnología de información no administra los generadores eléctricos, su acceso está a cargo del personal de operaciones del edificio. El personal de tecnología no tiene acceso físico a los generadores eléctricos

23. No se ha podido comprobar la frecuencia de la realización respaldos de la información y tampoco los procedimientos de comprobación de los mismos, no existen simulacros de pérdida de información y situaciones de entrenamiento para recuperación y utilización de respaldos.

24. No se ha podido evidenciar la existencia de manuales e informes entregados por los proveedores además de procedimientos de actualización de la información con la que se cuenta

25. Existe dependencia del personal técnico en ciertas áreas específicas, el personal de desarrollo no comparte el conocimiento ganado de la experiencia a un repositorio central o con sus compañeros.

26. No se identifica un sistema de gestión de incidencias ligado al inventario de equipo informático, las incidencias se administran mediante bitácoras manuales, no se realizan evaluaciones de calidad al servicio de soporte técnico ligados a la incidencia que es atendida.

27. No existe documentación que justifique una adecuada sociabilización de los riesgos y las actividades de mitigación de los mismos por parte de la dirección hacia los empleados directamente involucrados en los procesos críticos de la organización

28. Los riesgos no son medidos ni controlados, pero aun han sido detectados, pero aun se ha realizado actividades independientes para evaluarlos

5. Capítulo V

En este capítulo se establece el nivel de madurez basado en COBIT 4.1 de cada proceso en el área de tecnología recopilando la información generada hasta el momento y aportando con las observaciones y recomendaciones para una escalabilidad al próximo nivel.

5.1. Establecimiento del modelo de madurez con COBIT

Para determinar el nivel de madurez de cada proceso ha sido relacionado con su Dominio referente y en relación a la siguiente tabla:

Tabla 12

Procesos con Dominios Cobit

Cód	Proceso	Cobit 4	Dominio
P11-01	Adquisiciones Garantías Equipo Electrónico	AI3	Adquirir y Mantener Infraestructura Tecnológica
P11-02	Soporte Técnico	DS8	Administrar la Mesa de servicio y los incidentes
P11-03	Administración de Respaldos	DS4	Garantizar la Continuidad del servicio
P11-04	Administración Data Center	DS12	Administración del Ambiente Fisco
P11-05	Administración Redes LAN	DS12	Administración del Ambiente Fisco
P11-06	Administración Redes WAN	DS12	Administración del Ambiente Fisco
P11-07	Mantenimiento de Hardware	DS12	Administración del Ambiente Fisco
P11-08	Mantenimiento De Licencias	DS12	Administración del Ambiente Fisco
P11-09	Desarrollo y Mantenimiento de Aplicaciones	AI6	Administrar Cambio
P11-10	Administración de Servidores	DS12	Administración del Ambiente Fisco
P11-11	Administración de usuarios	PO07	Administrar los Recursos Humanos de TI

5.1.1. AI3 Adquirir y Mantener Infraestructura Tecnológica

Este Dominio contiene al proceso “Adquisiciones Garantías Equipo Electrónico (P11-01)” y trata que las organizaciones deban contar con procesos para adquirir,

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

5.1.1.1. Evaluación de los objetivos de control del proceso AI3: Administración de operaciones.

Tabla 13

Evaluación de los objetivos de control Dominio AI3

DOMINIO: AI3 ADQUIRIR Y MANTENER INFRAESTRUCTURA TECNOLÓGICA

OBJETIVO DE CONTROL	#	Pruebas del diseño de control	Calificación		Observaciones
			Obtenida	Total	
AI3.1 PLAN DE ADQUISICIÓN DE INFRAESTRUCTURA TECNOLÓGICA	1	Existe un plan para adquirir, Implementar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio, y que esté de acuerdo con la dirección tecnológica de la organización.	1	1	
	2	El plan considera extensiones futuras para adiciones de capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología.	0	1	
	3	Se puede evaluar los costos de complejidad y la viabilidad comercial del proveedor y el producto al añadir nueva capacidad técnica.	0	1	
AI3.2 PROTECCIÓN Y DISPONIBILIDAD DEL RECURSO DE INFRAESTRUCTURA	4	Se puede verificar que esta implementado medidas de control interno, seguridad y audibilidad durante la configuración, integración y Mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad.	1	1	
	5	Se deben definir y comprender claramente las responsabilidades al utilizar componentes de infraestructura sensitivos por todos aquellos que desarrollan e integran los componentes de infraestructura.	0,75	1	
	6	Se puede verificar que los recursos son monitoreados y evaluados.	1	1	

Continua

AI3.3 MANTENIMIENTO DE LA INFRAESTRUCTURA	7	Se puede verificar que existe desarrollada una estrategia y un plan de Mantenimiento de la infraestructura para garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización.	0,6	1
	8	Se puede confirmar que se realiza una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad	0,25	1
AI3.4 AMBIENTE DE PRUEBA DE FACTIB ILIDAD	4	Se puede verificar que existe el ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura, en las primeras fases del proceso de adquisición y desarrollo.	1	1
PUNTAJES:			3,75	6
PORCENTAJE DE CUMPLIMIENTO			**62,5**	

Porcentaje de cumplimiento del proceso: de las 4 pruebas de diseño de control que fueron evaluadas en el proceso AI3 Adquirir y Mantener Infraestructura Tecnológica, se obtienen 3,75 puntos de 6 posibles, para alcanzar un porcentaje de cumplimiento del 62,5%.

5.1.1.2. Modelo de madurez del proceso AI3: Adquirir y Mantener Infraestructura Tecnológica

Tabla 14

Modelo de Madurez del objetivo de control para el Dominio AI3

DOMINIO: AI3 ADQUIRIR Y MANTENER INFRAESTRUCTURA TECNOLÓGICA

NIVEL DE MADUREZ		**Descripción**	**Cumple**	**No Cumple**	**Observaciones**
0	NO EXISTENTE	Cuando la organización no dedica tiempo y recursos al establecimiento de soporte básico de TI y a actividades operativas.	X		
1	INICIAL	Cuando la organización reconoce la necesidad de estructurar las funciones de soporte TI. Se establecen algunos procedimientos estándar y las actividades de operaciones son de naturaleza reactiva.	X		

Continua

2	REPETIBLE PERO INTUITIVO	Cuando la organización esta consiente del rol clave que las actividades de operaciones TI juegan en brindar funciones de soporte de TI	X
3	DEFINIDO	Cuando se entiende y acepta dentro de la organización la necesidad de administrar las operaciones de cómputo. Se han asignado recursos y se lleva a cabo alguna habilitación durante el trabajo.	X
4	ADMINISTRADO Y MEDIBLE	Cuando las operaciones de cómputo y las responsabilidades de soporte están definidas de forma clara y la propiedad está asignada. Las operaciones se soportan a través de presupuestos de recursos para gastos de capital y de recursos humanos.	

5.1.2. AI6 Dominio Administrar Cambio

Este Dominio contiene al proceso P11-09 Desarrollo y Mantenimiento de Aplicaciones sobre el manejo todos los cambios, incluyendo el Mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formalmente y controlada. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previo a la implantación y revisar contra los resultados planeados después de la implantación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción

5.1.2.1. Evaluación de los objetivos de control del proceso AI6: *Administración de Cambios.*

Tabla 15

Evaluación de Objetivos de control para el Dominio AI6

DOMINIO: AI6 ADMINISTRAR CAMBIOS

OBJETIVO DE CONTROL	#	**Pruebas del diseño de control**	**Calificación**		**Observaciones**
			Obtenida	**Total**	

Continua

AI6.1 ESTÁNDARES Y PROCEDIMIENTOS PARA CAMBIOS	1	Se puede verificar que se encuentran establecidos procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes (incluyendo Mantenimiento y parches) para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio y las plataformas fundamentales	0,15	1	El proceso es claramente definido para cambios de requerimientos formales y no en correcciones o cambios de emergencia
AI6.2 EVALUACIÓN DE IMPACTO, PRIORIZACIÓN Y AUTORIZACIÓN	2	Se pude garantizar que todas las solicitudes de cambio se evalúan de una manera estructurada en cuanto a impactos en el sistema operacional y su funcionalidad. Esta evaluación deberá incluir categorización y priorización de los cambios. Previo a la migración hacia producción, los interesados correspondientes autorizan los cambios	0,10	1	El impacto es evaluado antes de realizar el cambio en el ambiente de desarrollo, pero solo de cambios significativos
AI6.3 CAMBIOS DE EMERGENCIA	3	Se encuentra establecido un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido. La documentación y pruebas se realizan posiblemente después de la implantación del cambio de emergencia	0,05	1	No existe un procedimiento formalmente documentado siendo la mayoría de cambios de emergencia sin documentación
AI6.4 SEGUIMIENTO Y REPORTE DEL ESTATUS DE CAMBIO	4	Esta establecido un sistema de seguimiento y reporte para mantener actualizados a los solicitantes de cambio y a los interesados relevantes, acerca del estatus del cambio a las aplicaciones, a los procedimientos, a los procesos, parámetros	0,45	1	El departamento cuenta con un Sistema de Requerimientos el cual refleja e informa el estado del requerimiento al usuario

Continua

		del sistema y del servicio y las plataformas fundamentales			
AI6.5 CIERRE Y DOCUMENTACIÓN DEL CAMBIO	5	Está formalmente definido que siempre que se implantan cambios al sistema, se debe actualizar el sistema asociado, la documentación de usuario y procedimientos correspondientes. Estableciendo un proceso de revisión para garantizar la implantación completa de los cambios	0,10	1	No toda la documentación de las aplicaciones se encuentra actualizada lo que dificulta registrar el cambio
PUNTAJES:			0,85	5	
PORCENTAJE DE CUMPLIMIENTO			**17,00**		

Porcentaje de cumplimiento del proceso: de los 5 objetivos de control que fueron evaluadas en el proceso AI6 ADMINISTRACIÓN DE CAMBIOS, se obtienen 0,85 DE 5 puntos, para alcanzar un porcentaje de cumplimiento del 17 %.

5.1.2.2. Modelo de madurez del proceso AI6: Administración de Cambios

Tabla 16

Modelo de Madurez del objetivo de control para el Dominio AI6

DOMINIO: AI6 ADMINISTRAR CAMBIOS

NIVEL DE MADUREZ	**Descripción**	**Cumple**	**No Cumple**	**Observaciones**
0 NO EXISTENTE	No existe un proceso definido de administración de cambio y los cambios se pueden realizar virtualmente sin control. No hay conciencia de que el cambio puede causar una interrupción para	X		

Continua

		TI y las operaciones del negocio y no hay conciencia de los beneficios de la buena administración de cambio	
1	INICIAL	Se reconoce que los cambios se deben administrar y controlar. Las prácticas varían y es muy probable que se puedan dar cambios sin autorización. Hay documentación de cambio pobre o no existente y la documentación de configuración es incompleta y no confiable. Es posible que ocurran errores junto con interrupciones al ambiente de producción, provocados por una pobre administración de cambios	X
2	REPETIBLE PERO INTUITIVO	Existe un proceso de administración de cambio informal y la mayoría de cambios siguen este enfoque; sin embargo el proceso no está estructurado, es rudimentario y propenso a errores. La exactitud de la documentación de la configuración es inconsistente y de planeación limitada y la evaluación de impacto se da previa al cambio	X

5.1.4. DS4 Dominio Garantizar la Continuidad del servicio

Este Dominio contiene al proceso P11-03 Administración de Respaldos relacionándose con la necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio

5.1.4.1. Evaluación de los objetivos de control del proceso DS4 Administración de operaciones.

Tabla 17

Evaluación de los Objetivos de Control Dominio DS4

DOMINIO: DS4 DOMINIO GARANTIZAR LA CONTINUIDAD DEL SERVICIO

OBJETIVO DE CONTROL	#	Pruebas del diseño de control	Calificación		Observaciones
			Obtenida	Total	
DS4.1 MARCO DE TRABAJO DE CONTINUIDAD DE TI	1	Preguntar y confirmar que un proceso de gestión de continuidad de negocio de toda la empresa este diseñado y aprobado por la administración a nivel ejecutivo.	0,75	1	Si tienen los procesos definidos para la operación de TI, sin embargo todos no están documentados.
	2	Determinar si el plan de continuidad del negocio tiene los recursos necesarios para recuperar las operaciones del negocio durante una interrupción.	1	1	
	3	Inspeccione el plan de continuidad del negocio para confirmar que incluye todos los elementos necesarios para reanudar el procesamiento del negocio en caso de una interrupción.	0,8	1	
DS4.2 PLANES DE	4	Compruebe que existan los planes de continuidad de negocio para todas las funciones y procesos más importantes del negocio.	0,8	1	

Continua

CONTINUIDAD DE TI	5	Revisar una muestra adecuada de los planes de continuidad de negocio y confirmar que:	0,75	1
		- Está diseñado para establecer la capacidad de recuperación.	0,8	1
		- Define las funciones y responsabilidades	0,75	1
		- Incluye los procesos de comunicación	0,5	1
		- Define la configuración de recuperación mínima aceptable.	0,6	1
	6	Obtener las pruebas de los planes de continuidad del negocio y la evidencia de que las pruebas se ejecutan con la frecuencia acordada.	1	1
	7	Revisar los resultados de las pruebas, y asegurar que las acciones resultantes son objeto de seguimiento.	0,65	1
DS4.3 RECURSOS CRÍTICOS DE TI	8	Obtener un listado de las funciones de la empresa con su respectiva criticidad del negocio y asegurarse de que existen planes de continuidad de las funciones de negocio más críticos.	0,45	1
	9	Revisar los planes para garantizar que están diseñados (y probados) para cumplir con los objetivos de negocio y los requisitos legales y reglamentarios.	0,7	1
	10	Determinar cómo se garantiza la coherencia entre los planes.	0,85	1
DS4.4 MANTENIMIENTO DEL PLAN DE CONTINUIDAD DE TI	11	Preguntar, y confirmar que todas las copias del plan de continuidad de TI estén actualizadas y se almacenan dentro y fuera de la oficina.	1	1
	12	Preguntar y confirmar que todos los cambios críticos en los recursos de TI se comunican con el gerente de TI.	1	1
	13	Preguntar y confirmar que los cambios en el plan de contingencia se hacen a intervalos apropiados siguiendo los procedimientos de control de cambios.	0,75	1
DS4.5 PRUEBAS DEL PLAN DE CONTINUIDAD DE TI.	14	Preguntar y confirmar que las pruebas de continuidad de TI están programadas y completadas en forma regular después de los cambios en la infraestructura de TI o de negocios y aplicaciones.	0,8	1
	15	Preguntar y confirmar que exista un calendario detallado de las pruebas, que incluya los detalles de la prueba y la cronología de eventos para garantizar una secuencia lógica y real.	1	1
	16	Preguntar a través de entrevistas si se evalúan los medios alternativos cuando una prueba no es factible de realizarla.	0,5	1
	17	Preguntar y confirmar que el éxito o el fracaso de las pruebas se midieron e informaron y si se realizan los cambio en el plan de continuidad de TI.	0,35	1
	18	Revisar los resultados y determinar la eficacia de su funcionamiento.	1	1
DS4.6 ENTRENAMIENTO DEL	19	Preguntar a través de entrevistas si se lleva a cabo regularmente el entrenamiento del plan de continuidad de TI.	0,75	1

Continua

PLAN DE CONTINUIDAD DE TI	20	Preguntar y confirman que las necesidades de capacitación y programas son evaluados y actualizados periódicamente.	0,5	1
	21	Revisión horarios y material de capacitación para determinar la eficacia.	0,35	1
	22	Preguntar si los programas de sensibilización del plan de continuidad de TI se están realizando a todos los niveles.	0,85	1
DS4.7 DISTRIBUCIÓN DEL PLAN DE CONTINUIDAD DE TI	23	Preguntar y confirmar que se ha creado una lista de distribución para el plan de continuidad de TI.	0,65	1
	24	Obtenga el procedimiento de distribución del plan de continuidad de TI.	0,6	1
	25	Evaluar el procedimiento y verificar su cumplimiento.	0,75	1
	26	Preguntar y confirmar que todas las copias digitales y físicas del plan están protegidas de forma adecuada y que los documentos son accesibles únicamente por personal autorizado.	1	1
DS4.8 RECUPERACIÓN Y REANUDACIÓN DE LOS SERVICIOS DE TI	27	Solicitar copia del proceso de gestión de incidentes, y asegúrese de que incluye los pasos para la evaluación de daños, así como los puntos de decisión formales y umbrales para activar los planes de continuidad.	0,25	1
	28	Revisar los planes de recuperación de TI, y confirmar que cumplen con los requerimientos del negocio.	0,85	1
DS4.9 ALMACENAMIENTO DE RESPALDOS FUERA DE LAS INSTALACIONES	29	Preguntar y confirman que los datos estén protegidos cuando se encuentran fuera de la oficina, mientras están en el transporte y cuando se encuentran en el lugar de almacenamiento.	0,5	1
	30	Preguntar y confirman que los servicios de apoyo no están sujetos a los mismos riesgos que en el sitio primario.	0,75	1
	31	Preguntar y confirmar que las pruebas de recuperación se realizan para garantizar la calidad de las copias de seguridad y medios.	0,8	1
	32	Revisar los procedimientos de las pruebas para determinar la eficacia.	0,9	1
	33	Verifique que los medios de las copias de seguridad contengan toda la información requerida por el plan de continuidad de TI.	1	1
	34	Preguntar y confirmar que existen instrucciones de recuperación y etiquetado de los medios.	0,2	1
	35	Preguntar y confirmar que existe un inventario de las copias de seguridad y de los medios.	1	1
DS4.10 REVISIÓN POST REANUDACIÓN	36	Preguntar y confirmar que las deficiencias del plan se han detectado y se han convertido en oportunidades de mejora.	0,6	1
	37	Revisar los planes, políticas y procedimientos para determinar la efectividad de la operación.	0,45	1
		PUNTAJES:	29,55	4

Continua

PORCENTAJE DE CUMPLIMIENTO	**72,07**

Porcentaje de cumplimiento del proceso: de las 41 pruebas de diseño de control que fueron evaluadas en el proceso D S4 ADMINISTRACIÓN DE OPERACIONES, se obtienen 29,55 de 41puntos, p ara alcanzar un porcentaje de cumplimiento del 72,07%.

5.1.4.2. Modelo de madurez del proceso Ds4:

Tabla 18

Modelo de Madurez del objetivo de control para el Dominio DS4

DOMINIO: DS4 DOMINIO GARANTIZAR LA CONTINUIDAD DEL SERVICIO

	NIVEL DE MADUREZ	**Descripción**	**Cumple**	**No Cumple**	**Observaciones**
0	NO EXISTENTE	No hay entendimiento de los riesgos, vulnerabilidades y amenazas a las operaciones de TI o del impacto en el negocio por la pérdida de los servicios de TI. No se considera que la continuidad en los servicios deba tener atención de la gerencia.	X		
1	INICIAL	Las responsabilidades sobre la continuidad de los servicios son informales y la autoridad para ejecutar responsabilidades es limitada.	X		
2	REPETIBLE PERO INTUITIVO	Se asigna la responsabilidad para mantener la continuidad del servicio. Los enfoques para asegurar la continuidad están fragmentados. Los reportes sobre la disponibilidad son esporádicos, pueden estar incompletos y no toman en cuenta el impacto en el negocio.	X		
3	DEFINIDO	La responsabilidad sobre la administración de la continuidad del servicio es clara. Las responsabilidades de la planeación y de las pruebas de la continuidad de los servicios están claramente asignadas y definidas.	X		

Continua

4	ADMINISTRADO Y MEDIBLE	Se hacen cumplir las responsabilidades y los estándares para la continuidad de los servicios. Se asigna la responsabilidad de mantener un plan de continuidad de servicios. Las actividades de Mantenimiento están basadas en los resultados de las pruebas de continuidad, en las buenas prácticas internas y en los cambios en el ambiente del negocio y de TI.	
5	OPTIMIZADO	Los procesos integrados de servicio continuo toman en cuenta referencias de la industria y las mejores prácticas externas. El plan de continuidad de TI está integrado con los planes de continuidad del negocio y se da Mantenimiento de manera rutinaria.	

5.1.5. DS 8 Dominio Administrar la Mesa de servicio y los incidentes

Este Dominio contiene al proceso Soporte Técnico (P11-02), Responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de TI, requiere de una mesa de servicio bien diseñada y bien ejecutada, de un proceso de administración de incidentes. Este proceso incluye la creación de una función de mesa de servicio con registro, escalamiento de incidentes, análisis de tendencia, análisis causa raíz y resolución. Los beneficios de negocio incluyen el incremento en la productividad gracias a la resolución rápida de consultas. Además, el negocio puede identificar la causa raíz (tales como un pobre entrenamiento a los usuarios) a través de un proceso de reporte efectivo

5.1.5.1. Evaluación de los objetivos de control del proceso DS8: Administración de operaciones.

Tabla 19

Evaluación de los Objetivos de Control Dominio DS8

DOMINIO: DS8 DOMINIO ADMINISTRAR LA MESA DE SERVICIO

OBJETIVO DE CONTROL	#	Pruebas del diseño de control	Calificación		Observaciones
			Obtenida	Total	
DS8.1 MESA DE SERVICIOS	1	Preguntar y confirmar que existe service desk de TI.	1	1	
	2	Preguntar y confirmar que se ha realizado un análisis para determinar el modelo de service desk así como el personal, las herramientas y la integración con otros procesos.	0,5	1	
	3	Asegúrese de que las horas de funcionamiento y el tiempo de respuesta satisfacen los requerimientos del negocio.	0,7	1	
	4	Preguntar y confirmar que los requerimientos tengan niveles de prioridad que permitan identificar el tiempo de resolución y procedimientos de escalamiento.	0,5	1	
	5	Las herramientas para la mesa de servicio se aplican de conformidad con las definiciones de servicio y los requisitos del OLAs y SLAs.	0,3	1	
DS8.2 REGISTRO DE CONSULTA DE CLIENTES.	6	Asegúrese de que los procesos y las herramientas están al alcance de los usuarios.	0,75	1	
	7	Confirmar que el proceso incluye flujo de trabajo para el manejo y el escalamiento de consultas de los clientes.	0,25	1	
	8	Revisar una muestra de consultas de los clientes abiertas y cerradas para comprobar el cumplimiento de los procesos y servicios.	1	1	
DS8.3 ESCALAMIENTO DE INCIDENTES	9	Existe un procedimiento para reportar incidentes y gestionar el escalamiento.	1	1	
	10	Confirmar la existencia de un proceso para asegurar que los registros de incidentes se actualizan para mostrar la fecha y hora de la asignación al personal de TI.	1	1	
	11	Los registros de incidentes se actualizan a lo largo del ciclo de resolución.	1	1	
DS8.4 CIERRE DE INCIDENTES	12	Preguntar y confirmar que se sigue un proceso para gestionar la resolución de cada incidente.	1	1	
	13	Preguntar y confirman que todos los incidentes resueltos tienen un registro detallado de todos los pasos para resolver los incidentes.	1	1	
DS8.5 ANÁLISIS DE TENDENCIAS	14	Preguntar y confirmar que exista un proceso para identificar e investigar más a fondo e informar sobre los	1	1	

Continua

	incidentes que han sobrepasado los plazos para la resolución.		
15	Preguntar y confirmar si existe un análisis de tendencias en los incidentes cuando se repiten y si existen patrones en común, para apoyar la identificación del problema.	0	1
16	Preguntar y confirmar si se realizan encuestas a los clientes para evaluar los niveles de satisfacción con el servicio prestado por la mesa de servicio.	0	1
17	Verifique si el análisis de las encuestas de satisfacción se utiliza para la mejora continua.	0	1
PUNTAJES:		11	17
PORCENTAJE DE CUMPLIMIENTO		**64,71**	

Porcentaje de cumplimiento del proceso: de las 17 pruebas de diseño de control que fueron evaluadas en el proceso DS8 ADMINISTRACIÓN LA MESA DE SERVICIO, se obtienen 11 de 17 puntos, para alcanzar un porcentaje de cumplimiento del 64,71%.

5.1.5.2. Modelo de madurez del proceso Ds8: Administrar la Mesa de Servicio

Tabla 20

Modelo de Madurez del objetivo de control para el Dominio DS8

DOMINIO: DS8 ADMINISTRAR LA MESA DE SERVICIO

NIVEL DE MADUREZ		**Descripción**	**Cumple**	**No Cumple**	**Observaciones**
0	NO EXISTENTE	Cuando no hay soporte para resolver problemas y preguntas de los usuarios.	X		
1	INICIAL	Cuando la gerencia reconoce que requiere un proceso soportado por herramientas y personal para responder a las consultas de los usuarios y administrar la resolución de incidentes.	X		
2	REPETIBLE PERO INTUITIVO	Cuando hay conciencia organizacional de la necesidad de una función de mesa de servicio y de un proceso de administración de incidentes.	X		

Continua

3	DEFINIDO	Cuando se reconoce y se acepta la necesidad de contar con una función de mesa de servicio y un proceso para la administración de incidentes.	X
4	ADMINISTRADO Y MEDIBLE	Cuando en todos los niveles de la organización hay un total entendimiento de los beneficios de un proceso de administración de incidentes y la función de mesa de servicio se ha establecido en las unidades organizacionales apropiadas	
5	OPTIMIZADO	Cuando el proceso de administración de incidentes y la función de mesa de servicio están bien organizados y establecidos y se llevan a cabo con un enfoque de servicio al cliente son expertos.	

5.1.6. DS12 Dominio Administración del Ambiente Fisco

Este Dominio contiene a los procesos

- P11-04 Administración Data Center
- P11-05 Administración Redes LAN
- P11-06 Administración Redes WAN
- P11-07 Mantenimiento de Hardware
- P11-08 Mantenimiento de Licencias
- P11-10 Administración de Servidores

La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos (sito), la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.

5.1.6.1. Evaluación de los objetivos de control del proceso DS12: Administración Del Ambiente Físico

Tabla 21

Evaluación de los Objetivos de Control Dominio DS12

DOMINIO: DS12 ADMINISTRACION DEL AMBIENTE FISICO

OBJETIVO DE CONTROL	#	Pruebas del diseño de control	Calificación		Observaciones
			Obtenida	Total	
DS12.1 SELECCIÓN Y DISEÑO DEL CENTRO DE DATOS	1	Se puede confirmar que: El centro de datos para los equipos informáticos han sido seleccionados de acuerdo con una estrategia tecnológica que cumpla con los requerimientos del negocio y una política de seguridad, teniendo en cuenta cuestiones tales como la posición geográfica y los riesgos	0.75	1	
DS12.2 MEDIDAS DE SEGURIDAD FÍSICA.	2	Se puede confirmar que: - Existe Una política que define y aplica medidas para el control de acceso. - El acceso limitado a los sitios sensibles de TI. - Los sitios de TI sensibles son discretos y no pueden ser fácilmente identificados desde fuera. - El diseño de las medidas de seguridad física tiene en cuenta los riesgos asociados con el negocio y la operación.	1	1	
DS12.3 ACCESO FÍSICO	3	Confirmar que: - Exista un proceso que rige la solicitud y concesión de acceso a las instalaciones de centro de datos. - Las solicitudes de acceso formales se han completado y autorizados por la administración de TI. - Hay un proceso para registrar y controlar todos los puntos de entrada al centro de datos de TI - Existe una política de instruir a todo el personal para mostrar identificación visible en todo momento y	1	1	

Continua

		evita la emisión de documentos de identidad o tarjetas sin la debida autorización. - Existe una política que exige a los visitantes ser acompañados en todo momento por un miembro del grupo de operaciones de TI		
DS12.4 PROTECCIÓN CONTRA FACTORES AMBIENTALES	4	Confirmar que: - Exista un proceso para identificar los desastres naturales y de origen humano que pueda ocurrir en la zona en la que se encuentran las instalaciones de TI. - Una política que describe cómo están protegidos los equipos informáticos contra el robo o amenazas ambientales.	0,6	1
DS12.5 ADMINISTRACIÓN DE INSTALACIONES FÍSICAS	5	Preguntar y confirmar que: - Exista un proceso que examine la necesidad de protección contra las condiciones ambientales e interrupciones de energía eléctrica. - Fuente de energía eléctrica ininterrumpida. - Pruebas periódicas del funcionamiento del UPS. - Sistema contra incendios. - Cableado se encuentra bajo tierra o tiene una protección alternativa adecuada. - Existen planos. - Cableado está protegido y reforzado contra riesgos ambientales. - Racks de cableado tienen acceso restringido. - Existe un proceso para educar al personal sobre las leyes, reglamentos o directrices de salud y seguridad. - El Mantenimiento se lleva a cabo sólo por personal autorizado	1	1
PUNTAJES:			3,6	5
PORCENTAJE DE CUMPLIMIENTO			**72,00**	

Porcentaje de cumplimiento del proceso: de las 5 pruebas de diseño de control que fueron evaluadas en el proceso DS12 ADMINISTRACIÓN DEL AMBIENTE FISICO, se obtienen 3,6 de 5 puntos, para alcanzar un porcentaje de cumplimiento del 72%.

5.1.6.2. Modelo de madurez del proceso Ds12: ADMINISTRACION DEL AMBIENTE FISICO

Tabla 22

Modelo de Madurez del objetivo de control para el Dominio DS12

DOMINIO: DS12 ADMINISTRAR AMBIENTE FISICO

NIVEL DE MADUREZ		**Descripción**	**Cumple**	**No Cumple**	**Observaciones**
0	NO EXISTENTE	Cuando no hay soporte para resolver problemas y preguntas de los usuarios.	X		
1	INICIAL	Cuando la gerencia reconoce que requiere un proceso soportado por herramientas y personal para responder a las consultas de los usuarios y administrar la resolución de incidentes.	X		
2	REPETIBLE PERO INTUITIVO	Cuando hay conciencia organizacional de la necesidad de una función de mesa de servicio y de un proceso de administración de incidentes.	X		
3	DEFINIDO	Cuando se reconoce y se acepta la necesidad de contar con una función de mesa de servicio y un proceso para la administración de incidentes.	X		
4	ADMINISTRADO Y MEDIBLE	Cuando en todos los niveles de la organización hay un total entendimiento de los beneficios de un proceso de administración de incidentes y la función de mesa de servicio se ha establecido en las unidades organizacionales apropiadas			
5	OPTIMIZADO	Cuando el proceso de administración de incidentes y la función de mesa de servicio están bien organizados y establecidos y se llevan a cabo con un enfoque de servicio al cliente son expertos.			

5.1.7. PO07 Dominio Administrar los Recursos Humanos de TI

Este Dominio contiene al proceso P11-11 Administración de usuarios

5.1.7.1. Evaluación de los objetivos de control del proceso PO07: Administración los Recursos Humanos de TI.

Tabla 23

Evaluación de los Objetivos de Control Dominio PO07

DOMINIO: PO07 ADMINISTRAR RECURSOS HUMANOS DE TI

OBJETIVO DE CONTROL	#	Pruebas del diseño de control	Calificación		Observaciones
			Obtenida	Total	
PO7.1 RECLUTAMIENTO Y RETENCIÓN DEL PERSONAL	1	Se puede asegurar que los procesos de reclutamiento del personal de TI estén de acuerdo a las políticas y procedimientos generales de personal de la organización (Ejemplo contratación un ambiente positivo de trabajo y orientación). La gerencia implementa procesos para garantizar que la organización cuente con una fuerza de trabajo posicionada de forma apropiada que tenga las habilidades necesarias para alcanzar las metas organizacionales.	1	1	
PO7.2 COMPETENCIAS DEL PERSONAL.	2	Se verifica de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y /o experiencia. Definir los requerimientos esenciales de habilidades para TI y verificar que se les de Mantenimiento usando programas de calificación y certificación según sea el caso	1	1	
PO7.3 ASIGNACIÓN DE ROLES	3	Definir, monitorear y supervisar los marcos de trabajo para los roles, responsabilidades y compensación del personal, incluyendo el requerimiento de adherirse a las políticas y procedimientos administrativos, así como al código de ética y prácticas profesionales. El nivel de	1	1	

Continua

		supervisión debe estar de acuerdo con la sensibilidad del puesto y el grado de responsabilidades asignadas		
PO7.4 ENTRENAMIENTO DEL PERSONAL DE TI	4	Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar su conocimiento, aptitudes, habilidades, controles internos y conciencia sobre la seguridad, al nivel requerido para alcanzar las metas organizacionales	0,75	1
PO7.5 DEPENDENCIA SOBRE LOS INDIVIDUOS	5	Minimizar la exposición a dependencias críticas sobre individuos clave por medio de la captura del conocimiento (documentación), compartir el conocimiento, planeación de la sucesión y respaldos del personal	0,5	1
PO7.6 PROCEDIMIENTOS DE INVESTIGACIÓN DEL PERSONAL	6	Incluir verificaciones de antecedentes en el proceso de reclutamiento de TI. El grado y la frecuencia de estas verificaciones dependen de que tan delicada o critica sea la función y se deben aplicar a los empleados, contratistas y proveedores	1	1
PO7.7 EVALUACIÓN DEL DESEMPEÑO DEL EMPLEO	7	Es necesario que las evaluaciones de desempeño se realicen periódicamente, comparando contra los objetos individuales derivados de las metas organizacionales, estándares establecidos y responsabilidades especificas del puesto. Los empleados deben recibir adiestramiento sobre su desempeño y conducta según sea necesario	1	1
PO7.8 CAMBIOS Y TERMINACIÓN DE TRABAJO	8	Tomar medidas expeditas respecto a los cambios en los puestos en especial las terminaciones. Se deben realizar la trasferencia del conocimiento, reasignar responsabilidades y se deben eliminar los privilegios de acceso, de tal modo que los riesgos se minimicen y se	0,25	1

Continua

	garantice la continuidad de las funciones		
PUNTAJES:		6,5	8
PORCENTAJE DE CUMPLIMIENTO		**81,25**	

Porcentaje de cumplimiento del proceso: de las 8 pruebas de diseño de control que fueron evaluadas en el proceso DS13 ADMINISTRACIÓN DE OPERACIONES, se obtienen 6,5 de 8 puntos, para alcanzar un porcentaje de cumplimiento del 81,25%.

5.1.7.2. Modelo de madurez del proceso PO07: Administrar Recursos Humanos de TI

Tabla 24

Modelo de Madurez del objetivo PO07Administrar Recursos Humanos de TI

DOMINIO: PO07 ADMINISTRAR RECURSOS HUMANOS DE TI

NIVEL DE MADUREZ		**Descripción**	**Cumple**	**No Cumple**	**Observaciones**
0	NO EXISTENTE	No existe conciencia sobre la importancia de alinear la administración de recursos humanos de ti con el proceso de planeación de la tecnología para la organización. No hay persona o grupo formalmente responsable de la administración de los recursos humanos de TI	X		
1	INICIAL	La gerencia reconoce la necesidad de contar con administración de recursos humanos de TI. El proceso de administración de recursos humanos de TI es informal y reactivo. El proceso de recursos humanos de TI está enfocado de manera operacional en la contratación y administración del personal de TI. Se está desarrollando la conciencia con respecto al impacto que tienen los cambios rápidos de negocio y de tecnología, y las soluciones cada vez más complejas, sobre la necesidad de nuevos niveles de habilidades y de competencia.	X		
2	REPETIBLE PERO INTUITIVO	Existe un enfoque táctico para contratar y administrar al personal de TI, dirigió por necesidades específicas de proyectos, en lugar de hacerlo	X		

Continua

		con base en un equilibrio entendido de disponibilidad interna y externa de personal calificado. Se imparte entrenamiento informal al personal nuevo, quienes después reciben entrenamiento según sea necesario	
3	DEFINIDO	Existe un proceso definido y documentado para administrar los recursos humanos de TI. Existe un plan de administración de recursos humanos. Existe un enfoque estratégico para la contratación y administración del personal de TI. El plan de entrenamiento formal está diseñado para satisfacer las necesidades de los recursos humanos de ti. Está establecido un programa de rotación, diseño para expandir las habilidades gerenciales y de negocio	X
4	ADMINISTRADO Y MEDIBLE	La responsabilidad de la elaboración y el Mantenimiento de un plan de administración de recursos humanos para TI han sido asignados a un individuo o grupo con las habilidades y experiencia necesaria para elaborar y mantener el plan. El proceso para elaborar y mantener el plan de administración de recursos humanos de TI responde al cambio. La organización cuenta con métricas estandarizadas que le permiten identificar desviaciones respecto al plan de administración de recursos humanos de Ti con énfasis especial en el manejo del crecimiento y rotación dl personal. Las revisiones de compensación y de desempeño se están estableciendo y se comparan con otras organizaciones de TI y con las mejores prácticas de la industria. La administración de recursos humanos es proactiva, tomando en cuenta el desarrollo de una plan de carrera	X

Continua

5	OPTIMIZADO	El plan de administración de recursos humanos de ti se actualiza de forma constante para satisfacer los cambiantes requerimientos del negocio. La administración de recursos humanos de TI está integrada y responde a la dirección estratégica de la entidad. Los componentes de la administración de recursos humanos de ti son consistentes con las mejores prácticas de la industria, tales como adiestramiento. Los programas de entrenamiento se desarrollan para todos los nuevos estándares tecnológicos y productos antes de su implantación en la organización

5.2. Resumen de los niveles de Madurez por Dominio

Para determinar los niveles de madurez se han agrupado cada uno de ellos en la siguiente tabla

Tabla 25

Porcentaje de Nivel de Madurez por Dominio

CONSOLIDADO DE NIVELES DE MADUREZ POR DOMINIO

DOMINIO	**Nivel de madurez**	**Nivel de cumplimiento**
AI3 Adquirir Y Mantener Infraestructura Tecnológica	3	62,5
AI6 Administrar Cambios	0	17
DS4 Dominio Garantizar La Continuidad Del Servicio	3	72,07
DS8 Dominio Administrar La Mesa De Servicio	3	64,71
DS12 Administración Del Ambiente Físico	3	72
P007 Administrar Recursos Humanos De Ti	4	81,25

En la figura 6, se muestra el nivel de madurez alcanzado durante la evaluación de la auditoría del dominio entregar y dar soporte por cada proceso.

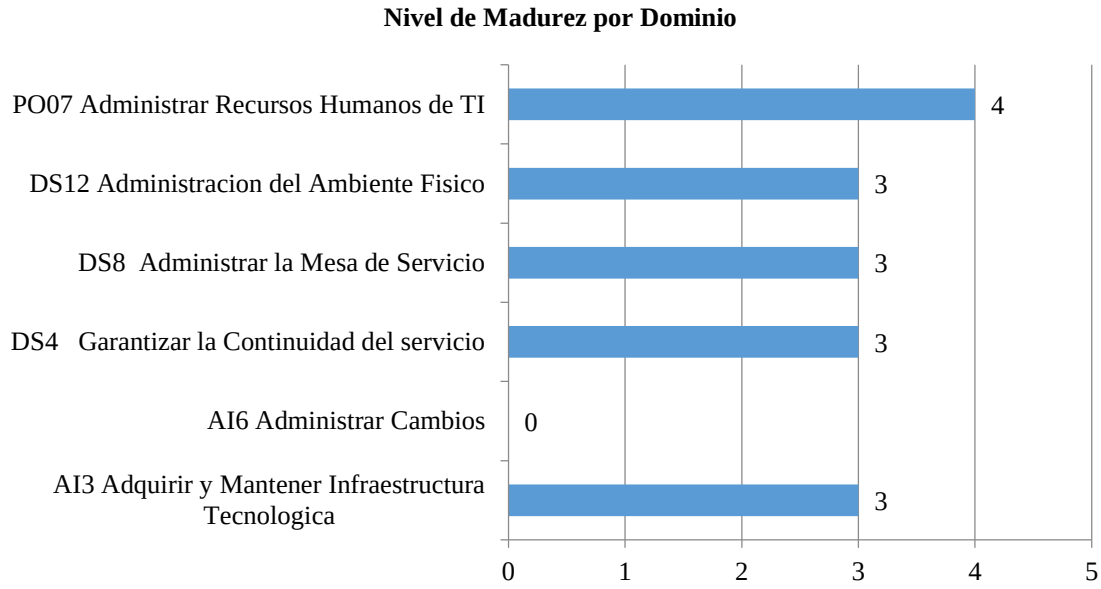


Figura 6: "Nivel de madurez por dominio"

El Departamento de TI obtiene el nivel de madurez más bajo con 0 (cero) en el procesos AI6 y el nivel de madurez 3 en los procesos DS12, DS8, DS4, AI3, y el nivel más alto 4 (cuatro) en el proceso PO07.

El departamento de TI no obtiene ningún proceso en los niveles de madurez 1 (uno) y 5 (cinco), lo cual permite alertar sobre la administración y cumplimiento de los procesos.

En la figura 7, se muestra los niveles de madurez por el porcentaje de cumplimiento

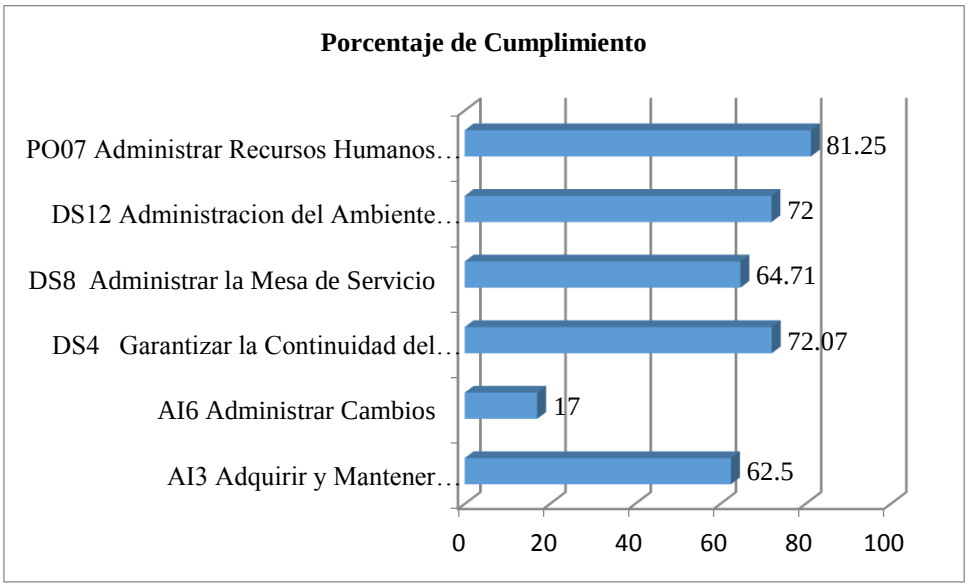


Figura 7: "Porcentaje de cumplimiento"

De la tabulación de los resultados obtenidos se puede obtener la tabla de madurez, que muestra la cantidad de procesos que se ubican en determinado grado de madurez.

Tabla 26

Consolidado Nivel de Madurez por Dominio

NIVEL DE MADUREZ	PROCESOS
NIVEL 0	1
NIVEL 1	0
NIVEL 2	0
NIVEL 3	4
NIVEL 4	1
NIVEL 5	0

En la figura 8, se muestra que fueron auditados los 13 procesos del domino Entregar y Dar Soporte, del total de seis procesos se ubicaron en el nivel de madurez 1, cuatro procesos en el nivel de madurez 2, tres procesos en nivel de madurez 3. Podemos notar que ningún proceso se ubicó en el nivel de madurez cuatro y cinco.

Determinación de las Recomendaciones de madurez

RESUMEN GENERAL DEL NIVEL DE MADUREZ POR LOS DOMINIOS ACTUALES

Codigo	DOMINIO	NO EXISTENTE	INICIAL	REPETIBLE PERO INTUITIVO	DEFINIDO	ADMINISTRADO Y MEDIBLE	OPTIMIZADO
		0	1	2	3	4	5
AI3	Adquirir y Mantener Infraestructura Tecnologica						
AI6	Administrar Cambio						
DS4	Garantizar la Coninuidad del servicio						
DS8	Administrar la Mesa de servicio y los incidentes						
DS12	Administracion del Ambiente Fisco						
PO07	Administrar los Recursos Humanos de TI						

Figura 8: “Recomendaciones de madurez”

6. Capítulo VI

6.1. Desarrollo del Proceso de Auditoria (6.0)

6.1.1. Informe de Auditoria al área de Tecnología de Tecniseguros S.A.

En cumplimiento de la auditoría realizada en Tecniseguros S.A. en el área de tecnología de información y teniendo en cuenta los principios de control interno, se lleva a cabo la lectura y se presenta el informe preliminar.

Objetivo

Verificar las actividades realizadas en el área de tecnología de información de Tecniseguros S.A. mediante la metodología de análisis de riesgos.

Alcance

Revisar y Constatar las acciones tomadas en los 11 procesos del área de tecnología de Tecniseguros S.A.

Periodo de Cobertura

El proceso de auditoria se realizó en el periodo desde el 27 de Agosto 2013 hasta el 28 de Marzo 2014, fecha en la cual se realizó la lectura y entrega del documento final.

Metodología

En el proceso de consolidación de la información para realizar el proceso de la auditoría se realizaron actividades de:

- Identificación de los procesos del área de tecnología.
- Analizar los procesos desde el punto de vista de riesgos mediante el marco de referencia COSO ERM.
- Identificar los riesgos de cada proceso mediante Magerit.

- Cuantificar el riesgo en cada componente del cubo de COSO:
- Entorno de control
- Planteamiento de objetivos
- Identificación de eventos
- Evaluación de riesgos
- Actividades de control
- Información y comunicación
- Supervisión y monitoreo

Antecedentes

Tecniseguros cuenta con 280 empleados de los cuales 175 trabajan en la Regional de Quito bajo la dirección de la Gerencia Regional.

Tecniseguros creció bajo el ejemplo de disciplina de sus fundadores y directores, quienes han generado un ambiente de negocios ético y constructivo a lo largo del tiempo. Este progreso no sería posible sin la razón de ser de Tecniseguros que son sus clientes, muchos de los cuales le acompañan por más de 30 años con su fidelidad.

A partir de Tecniseguros nació el Grupo Futuro, manteniendo un crecimiento económico sostenible, generando fuentes de trabajo e invirtiendo en el país con capital nacional.

El Grupo Futuro está conformado por: Tecniseguros S.A., el mayor corredor de seguros del país; Seguros Equinoccial, empresa líder en seguros patrimoniales; Salud S.A. pionera en el ámbito de la medicina prepagada; Equivida S.A., la primera compañía de seguros de vida y Metropolitan Touring que con más de 50 años de trayectoria es la más importante empresa de turismo del país.

El departamento de tecnología está considerado una fortaleza y elemento de apoyo la organización siendo el responsable del manejo de la información y aplicaciones

necesarias el trabajo con los clientes, siendo una característica diferenciadora el desarrollo interno de aplicaciones,

El Departamento de Tecnología cuenta con la siguiente estructura:

Gerente de Tecnología: Ejecutivo CIO de la empresa a cargo de los y temas de gobierno con participación en el comité ejecutivo.

Atención a Usuarios: Ejecutivo responsable del soporte a los usuarios siendo el primer filtro ante fallas y errores reportados.

Administrador de Infraestructura: Ejecutivo Responsable de la Administración de los servidores, redes, respaldos y servicio de correo.

Administrador de Base de Datos: Ejecutivo responsable del monitoreo de las réplicas de las bases de datos a nivel nacional, así como la administración y Mantenimiento de la misma, verificando la integridad y estándar en la nomenclatura.

Ejecutivo de Apoyo GYE: Ejecutivo responsable del soporte a los usuarios siendo el primer filtro ante fallas y errores reportados, apoyando en el área de desarrollo para aplicaciones contables.

Administrador Control de Calidad: Ejecutivo Responsable del Análisis, Diseño y coordinación del desarrollo de las aplicaciones supervisando el desarrollo de los programadores, así como también responsable del versiona miento de las fuentes y puesta en producción de los aplicativos a nivel nacional

Programador: Ejecutivo responsable del desarrollo de aplicaciones Windows y Web según los requerimientos asignados realizando la documentación técnica y manual de usuario.

Procesos a cubrir

- Adquisiciones Garantías Equipo Electrónico
- Soporte Técnico
- Administración de Respaldos
- Administración Data Center
- Administración Redes LAN
- Administración Redes WAN
- Mantenimiento de Hardware
- Mantenimiento De Licencias
- Desarrollo y Mantenimiento de Aplicaciones
- Administración de Servidores
- Administración de usuarios

En total, la auditoria comprendió once procesos, los cuales quedaron documentados en los capítulos 3 y 4 del documento de tesis.

RESULTADOS

Los resultados encontrados están orientados en los riesgos que tienen los procesos.

Con base en el desarrollo de la auditoria se determinaron doce (12) observaciones.

Observación 1

No existen políticas para manejar los riesgos a presentarse, por parte de la gerencia no se han emitido documentos formales que indiquen como proceder

Efecto

El personal de Tecniseguros no sabe cómo responder ante los riesgos, no existen planes de entrenamiento, o campañas de socialización de la respuesta a los riesgos.

Probabilidad = 3

Impacto = 5

Recomendaciones

Realizar campañas de educación para que los colaboradores de la empresa sepan cómo responder a los riesgos.

Observación 2

Tecniseguros no cuenta con una política de manejo de riegos para el área de TI.

El personal de Tecniseguros no tiene conocimiento sobre los riesgos existentes en su trabajo, ya que los riesgos son generales pero no específicos.

La cultura de riesgo de Tecniseguros S.A. no es conocida por todo el personal, existen personas que tienen interpretaciones diferentes de los riesgos que plantea la directiva.

Efecto

El área de TI no trabaja en función a los riesgos, mismos que no son formalmente conocidos dentro del área. Los objetivos del área están orientados a los requerimientos de la cotidianidad y no responden a un plan.

Los trabajadores pueden responder de manera caótica frente a acontecimientos que constan en los planes de riesgo, los impactos pueden ser mayores a los esperados por la organización.

Probabilidad = 3

Impacto = 4

Recomendaciones

Revisar la estructura del área de TI, determinar sus riesgos y cambiar el manejo de la misma. Socializar los riesgos y las respuestas a los mismos.

Fortalecer la política de comunicación de la cultura de riesgo, realizar ejercicios, evaluaciones y motivar el aprendizaje con recompensas y reconocimientos a las personas que los conozcan.

Observación 3

No se ha podido evidenciar que exista documento alguno que norme los procesos de reclutamiento, creación de cuentas, roles y privilegios de personal, para ninguna de las unidades administrativas de Tecniseguros. Ni aun para el área de TIC´s.

La asignación de privilegios está relacionada a perfiles de usuario y no a las identidades de cada persona. Los privilegios se asignan individualmente en cada aplicación, la tarea está a cargo, generalmente, del administrador del sistema. No se observan actividades de conciliación y reconciliación de usuarios en las aplicaciones y recursos informáticos.

No se encuentran controles que permitan conocer el uso o abuso de las cuentas privilegiadas de los sistemas, tales como root, admin, etc.

Efecto

Las tareas de aprovisionamiento son ejecutadas de manera manual y por el administrador de los sistemas. Existen cambios de privilegios de usuarios de manera no autorizada, acceso a funciones superiores y prohibidas. No existe una adecuada segregación de funciones. Pueden existir cuentas huérfanas en los recursos, mismas que podrían convertirse en fuentes de ataques.

No se puede auditar a los usuarios privilegiados, pérdida de responsabilidad individual.

Probabilidad = 3

Impacto = 3

Recomendaciones

Revisar los perfiles de los usuarios en cada uno de los recursos, buscar inconsistencia en los perfiles, cuentas con privilegios elevados, cuentas huérfanas, etc.

Mantener un repositorio centralizado de usuarios, miso que se encuentre integrado a los diferentes recursos informáticos.

Cambiar el modelo de gestión de usuarios de, perfiles a roles, permitiendo administrar a las personas con sus cargos y no sus perfiles en las aplicaciones.

Implementar un sistema de administración de identidades, mismo que permitirá gestionar de manera centralizada a las personas de la institución, generando automáticamente los accesos con los permisos necesarios de acuerdo a su rol dentro de la organización.

Implementar un sistema de monitoreo o administración de identidades privilegiadas, de modo que, se conozcan las actividades de estas cuentas y no se pierda la auditoría individual de cada persona en los diferentes recursos informáticos.

Observación 4

El control para el Mantenimiento y desarrollo de software es insuficiente, se detectan falencia en el proceso, fallas en el entregable y alto desarrollo de aplicaciones y pases a producción.

No existen ambientes separados de Desarrollo, pruebas y control de calidad.

Los datos que manejados por los desarrolladores son idénticos a los de producción, no están encriptados, o enmascarados.

Efecto

El proceso de desarrollo y Mantenimiento de aplicaciones no es coherente en toda la ejecución, existen fallas en los entregables, no se realizan las pruebas necesarias antes de liberar una aplicación, las pruebas y control de calidad se realizan en los equipos de los desarrolladores y no en ambientes especializados.

Probabilidad = 3

Impacto = 5

Recomendaciones

Crear los ambientes de pruebas y control de calidad, estos ambientes serán usados para evaluar las aplicaciones antes de su pase a producción, también contendrán los datos necesarios para su evaluación, corrección y mejora.

Enmascarar los datos de producción antes de pasarlo a los ambientes de pruebas y control de calidad, evitando que los desarrolladores y probadores tengan acceso a datos reales.

Observación 5

No se identifican equipos de red perimetral orientados a la función de IPS, es decir, no existen equipos de prevención de intrusiones. La única profesión es la de un firewall y el filtrado que brinda el canal de los proveedores.

Efecto

Múltiples ataques conocidos pueden llevarse a cabo de manera exitosa, tales como SQL Inyección, DOS, Cross site scripting, entre otros. Estos ataques se los puede obtener a través de programas de análisis de vulnerabilidades o test de penetración gratuitos en internet, no se requiere de mucha experiencia para ejecutar con éxito un ataque de este tipo.

Las aplicaciones pueden dejar de funcionar o experimentar un rendimiento degradado.

Probabilidad = 4

Impacto = 5

Recomendaciones

Implementar equipos de seguridad perimetral e internos que prevengan este tipo de ataques. Los equipos con funcionalidad de IPS específica se recomiendan sobre los UTM de propósito general.

Observación 6

Existe un ecosistema de diferentes soluciones, desarrolladas a medida, con diferentes bases de datos, y sin un control de crecimiento. Existen adaptaciones de las aplicaciones que responden a la cotidianidad y no al plan estratégico de la organización o planes de Tecniseguros S.A. Las aplicaciones están desarticuladas, no integradas y cada una sirve para un propósito específico. No existe un estándar en las herramientas de desarrollo utilizadas ni en las bases de datos. Existe mucho trabajo de operación y desarrollo en el área de tecnología, tampoco existe un repositorio centralizado de código fuente y ejecutables liberados.

Los pases a producción no se realizan con las pruebas necesarias. Las mismas personas de desarrollo realizan las pruebas de calidad. Existe embotellamiento en la persona de control de calidad por la cantidad de pases a producción. No existe un repositorio centralizado de las versiones de los programas.

Efecto

Falla total o parcial de los sistemas, tiempos de recuperación mayores a los esperados por el negocio, Incompatibilidad de aplicaciones, de lenguajes de programación y bases de datos, Dependencia de los desarrolladores expertos o experimentados, Tiempos elevados para dar respuesta a requerimientos.

Probabilidad = 3

Impacto = 4

Recomendaciones

Hacer una reingeniería de sistemas y evaluar la posibilidad de integrarlas en sistemas de mayor tamaño.

Definir un plan de desarrollo para los próximos 3 años, en donde se mencionen los lineamientos para los desarrollos futuros.

Construir o adaptar una arquitectura de aplicaciones para estandarizar los sistemas.

Observación 7

No existe evidencia de haber realizado un ataque controlado a la infraestructura de Tecniseguros, o un Ethical hacking en busca de vulnerabilidades. Esto podría generar el robo o alteración de información confidencial, bloqueo de los servicios y demás inconvenientes que pueden generar graves consecuencias

Efecto

No existe conciencia sobre la situación actual de las aplicaciones y de la infraestructura tecnológica de Tecniseguros, las vulnerabilidades se mantienen hasta que sean explotadas.

Probabilidad = 2

Impacto = 4

Recomendaciones

Realizar un análisis de vulnerabilidades a las aplicaciones y a la infraestructura.

Observación 8

No existen mecanismos de control de robo o adulteración de la información de los usuarios y clientes. No se identifican equipos o sistemas dedicados a evitar la fuga de información o cambios no autorizados.

Efecto

Los datos no están asegurados contra robo o alteración no autorizada.

Probabilidad = 2

Impacto = 5

Recomendaciones

Implementar políticas de control de datos o un sistema de prevención de pérdida de datos.

Observación 9

Las bitácoras de los sistemas, logs, flujos de red, y demás evidencia que arrojan los sistemas no se concentran en un repositorio único, haciendo que las aplicaciones dependan de especialistas para la interpretación de errores o eventos anormales. No es posible garantizar el análisis forense en base a las bitácoras en caso de ocurrir. No existe personal designado a revisar las bitácoras de los sistemas únicamente se revisan las bitácoras cuando existen inconvenientes.

Efecto

Cada aplicación guarda sus bitácoras o logs en su propio almacenamiento, el acceso y resguardo de esta información está a cargo del especialista de cada aplicación por lo que no existe una adecuada segregación de funciones.

Los logs pueden borrarse o modificarse sin que nadie se entere, perdiendo información que permita dar con el origen de los eventos inusuales.

Probabilidad = 2

Impacto = 4

Recomendaciones

Implementar un equipo que concentre los logs y demás bitácoras en un solo equipo, que permita la conciliación de estos, evitando que existan personas responsables de esta actividad. Tener un plan de manejo de Logs y bitácoras que garantice su normal operación.

Observación 10

El personal de tecnología de información no administra los generadores eléctricos, su acceso está a cargo del personal de operaciones del edificio. El personal de tecnología no tiene acceso físico a los generadores eléctricos

Efecto

Las personas encargadas de mantener la continuidad de las operaciones tecnológicas no pueden verificar el estado de los generadores, así como, su capacidad, nivel de combustible, entre otros. Las operaciones pueden detenerse debido a la falta de coordinación o comunicación entre estas dos partes.

Probabilidad = 2

Impacto = 3

Recomendaciones

El equipo de tecnología debe administrar los generadores eléctricos y garantizar la continuidad de los servicios tecnológicos. Actualizar la política de gestión de energía con los nuevos actores.

Observación 11

No se ha podido comprobar la frecuencia de la realización respaldos de la información y tampoco los procedimientos de comprobación de los mismos, no existen simulacros de pérdida de información y situaciones de entrenamiento para recuperación y utilización de respaldos.

Efecto

El personal no está entrenado para enfrentar un evento real. No se conoce el estado, utilidad y tiempo de respuesta de los respaldos de información. El tiempo de

recuperación y la pérdida de datos pueden superarlos umbrales esperados por Tecniseguros S.A.

Probabilidad = 2

Impacto = 3

Recomendaciones

Preparar planes de simulacro de fallos de sistemas, evaluar la calidad de los respaldos, definir procedimientos para responder en caso de un evento de desastre. Ejecutar simulacros con los sistemas críticos y no críticos al menos una vez al año. Definir responsables de cada actividad. Definir el protocolo de comunicación entre las partes operativas.

Observación 12

Existe dependencia del personal técnico en ciertas áreas específicas, el personal de desarrollo no comparte el conocimiento ganado de la experiencia a un repositorio central o con sus compañeros.

Efecto

Los procesos ligados a las aplicaciones tienen dependencia directa con una persona, misma que no tiene un control superior que valide lo que hace. Si una persona experta del equipo falta, renuncia o no tiene disponibilidad de tiempo el proceso puede detenerse o verse afectado en algún modo.

Probabilidad = 3

Impacto = 4

Recomendaciones

Generar campañas de transferencia de conocimiento entre el personal del área de tecnología, permitiendo tener personas con experiencia multidisciplinaria, capaces de responder a casi todos los incidentes que se reporten. Centralizar el conocimiento en

un lugar fuera de los propios técnicos, por ejemplo, una base de conocimientos administrada por el gerente del área.

Generar una política de transferencia de conocimiento entre los técnicos. Hacerla cumplir y evaluarla periódicamente para tener un mejoramiento continuo.

Observación 13

No se identifica un sistema de gestión de incidencias ligado al inventario de equipo informático, las incidencias se administran mediante bitácoras manuales, no se realizan evaluaciones de calidad al servicio de soporte técnico ligados a la incidencia que es atendida.

Efecto

Las personas comenten equivocaciones y las incidencias pueden ser olvidadas, tratadas fuera de tiempo, y no cumplir con los niveles de servicio acordados. La práctica del servicio no está orientada a la calidad, sino, al resultado, la experiencia del usuario puede ser negativa.

Probabilidad = 2

Impacto = 3

Recomendaciones

Implementar un sistema de administración de incidencias que cuente con un inventario, de modo que, sea capaz de tener el control de las incidencias atendidas por soporte, conocer los equipos que más incidencias han presentado, tener estadísticas de incidencias por unida de tiempo, de negocio y otros filtros.

Evaluar la calidad del servicio de soporte técnico brindado por el área y ligarlo a la incidencia, de esa manera será posible evidenciar la calidad del servicio y por ende, podrá ser mejorado.

Firmas

Representante del Área Auditada:

_____

Miroslava Aguirre

Gerente Nacional de Tecnología

Equipo Auditor:

_____	_____
Ing. Julio César Calderón Carrasco.	Ing. David Adolfo Ocaña Aldaz.
1716083876	1720437605

6.2.Informe ejecutivo de Auditoria

Objetivo:

Realizar una auditoría informática basada en el análisis de riesgos.

Alcance:

Revisar y Constatar las acciones tomadas en los 11 procesos del área de tecnología de Tecniseguros S.A.

Resultados:

De los resultados obtenidos se puede determinar que luego de la auditoría informática se detectó que el departamento de TI de la empresa Tecniseguros S.A obtiene un 42% en el cumplimiento de los procesos del Dominio DS1 Entregar y Dar Soporte. Esto evidencia que no existe un adecuado gobierno de TI que permita una correcta gestión de los recursos y servicios de TI.

Existen procesos y políticas que no se encuentran correctamente documentadas, la única persona que conoce de su existencia y ubicación es el Jefe de TI.

El jefe de TI, es el responsable del departamento de TI, asignando 4 principales funciones: Soporte a Usuarios, Administrador de infraestructura, Administrador de base de Datos, Desarrollo de Aplicaciones para lograr un apropiado gobierno de TI.

La empresa Tecniseguros S.A. no cuenta con un plan de contingencia para el departamento de TI, lo que puede causar serios problemas en la continuidad del negocio y en la toma de decisiones estratégicas frente a la competencia y el servicio a sus clientes.

Tras verificar estas y otras deficiencias se procede a emitir una serie de acciones sugeridas para que el departamento de TI pueda alcanzar un nivel de madurez 2 y 3 las mismas que se encuentran en el informe de auditoría detallado, pág. (64-78).

Recomendaciones de la Auditoría:

- Una vez concluida la auditoría se determina que el departamento de TI de la empresa Tecniseguros S.A, alcanza un nivel de madurez bajo, considerando que la naturaleza de la empresa es brindar servicios de: soporte, Mantenimiento e integración de soluciones tecnológicas, por lo que se recomienda implementar todas las recomendaciones que se incluyen en el informe de auditoría detallado, pág. (64-78).

- Para un adecuado Gobierno TI, el departamento de sistemas de la empresa Tecniseguros S.A, debe contar con propia autonomía y no depender de ninguna área si no reportar directamente al Director General de la empresa.

- Para minimizar las vulnerabilidades y amenazas de los activos del departamento de sistemas es de alta prioridad que se elabore el plan de contingencia, dentro del cual debe incluir un sitio alterno para el data center en las oficinas de Tecniseguros S.A. en la ciudad de Guayaquil.

6.3. Lectura del Informe

Se realizó varias sesiones de trabajo con el personal de las áreas auditadas donde se presentara el informe detallado a ser redactado, mismo que se ha puesto a consideración del Gerente de Tecnología

6.4. Presentación del Documento Definitivo

Si durante la lectura del borrador hay observaciones se las considerara caso contrario se realizara el informe definitivo mismo que se entregara a la máxima autoridad de la organización afín de que tome las medidas pertinentes para solucionar los errores detectados.

7. Capítulo VII

7.1. Conclusiones

- La metodología COSO ERM está enfocada en la administración de riesgos de toda la organización, se pueden analizar todas las unidades de negocio de manera independiente, y permite tener control total sobre todos los riesgos de una organización. En el caso de Tecniseguros S.A. permitió identificar y darle tratamiento a los riesgos, aunque los valores de ponderación son elegidos por los auditores.
- La metodología Magerit 3.0 está enfocada en identificar los activos de cada proceso, y de esta manera busca los riesgos en cada uno de ellos, el auditor y el equipo de riesgos son quieren determinan cuál puede aplicarse o cual no.
- El modelo de madurez de COBIT 4.1 está enfocado en los procesos, en el caso de Tecniseguros, existieron resultados inquietantes, los niveles de madures son relativamente altos, aun cuando, los procesos tenían riesgos, la principal razón es que, si bien existen procesos definidos, no se puede identificar si el proceso se cumple, si recae en personas específicas o en tecnología.
- Se identifican 28 riesgos, algunos de ellos se derivan de un único origen, como por ejemplo, la ausencia de equipos de seguridad perimetral que prevengan el ataque de intrusos no autorizados, es por eso que, las observaciones suelen ser menores a los riesgos encontrados.
- Al inicio de la auditoría se mencionó que, según el valor del riesgo, podía ubicarse en el cuadrante de evitar, es decir, eliminar las tareas relacionadas a esas áreas, sin embargo en la práctica, Tecniseguros S.A. no puede eliminar esas prácticas de manera inmediata, ya que son parte del negocio, en este caso lo que se recomienda es aplicar controles, es decir, dar un tratamiento similar al cuadrante de mitigar.
- Los valores de las ponderaciones utilizadas en esta auditoría son elegidos por los auditores y por la empresa auditada, es decir, para futuras auditorías pueden variar, con el objetivo de ser más o menos específicos.

7.2. Recomendaciones

- El modelo de madurez debe evaluarse en función de las personas, procesos y tecnología, en esta auditoría existieron puntos que identificaban que un proceso está maduro, sin embargo, la totalidad de las tareas recaen en personas, y si esas personas dejan la organización o el rol actual, corre el riesgo de detenerse, mientras que si la distribución estuviera orientada a procesos a tecnología el riesgo sería menor.
- Los procesos de administración de redes LAN y WAN deben tratarse como uno solo.
- El informe de auditoría debe ser usado como línea base para generar un línea base de proyectos, mismos que están orientados a mitigar los riesgos identificados, la prioridad la puede dar la organización o el jefe del área de tecnología.
- Para realizar una auditoría informática se recomienda utilizar como marco de referencia un Framework, que permite una evaluación de los procesos de TI a detalle, ya que cuenta con objetivos de control claros los cuáles son evaluados y analizados con una serie de pruebas de diseño de control en el transcurso de la auditoría, esto permite obtener un mejor resultado para establecer el correcto grado de madurez de cada proceso.
- Cuando se requiera construir una matriz de riesgos del departamento de TI se recomienda usar un estándar internacional ISO, el cual permite identificar claramente las debilidades y amenazas de los activos de TI, esto permite obtener una evaluación del riesgo mucho más precisa.
- Se recomienda implementar las mejores prácticas de ITIL en los procesos del departamento de sistemas, para garantizar la continuidad del negocio y minimizar los riesgos de seguridad informática.
- Se recomienda llevar una bitácora de evaluación de auditoría por cada proceso que debe ser firmada por el auditor y el auditado, para llevar una constancia por escrito de las evidencias encontradas y la aceptación de las mismas.
- Con respecto a la Auditoría realizada, se recomienda en un mediano plazo realizar la evaluación de los dominios de Cobit que no fueron parte de este proyecto: Planear y organizar, Adquirir e implementar, Monitorear y evaluar.

Bibliografía

Actiweb. (27 de 08 de 2013). *http://www.actiweb.es/msucreseccion29infysis/*. Obtenido de http://www.actiweb.es/msucreseccion29infysis/

Association, I. I. (14 de 08 de 2013). *Isaca*. Obtenido de http://www.isaca.org

Electrónica, C. S. (31 de Julio de 2014). *Consejo Superior de Administración Electrónica*. Obtenido de http://administracionelectronica.gob.es/pae_Home?_nfpb=true&_pageLabel=P80029225129365155099 1&langPae=es&detalleLista=PAE_1276529683497133#.U9sQee_Qdow

Guerra, M. (27 de 8 de 2013). *http://www.pwc.com/cl/es*. Obtenido de http://www.pwc.com/cl/es/cursos/finanzas-y-analisis-cuantitativo/coso-ii-enfoque-para-administracion-corporativa-de-riesgos.jhtml

IBM. (2012). IBM Security Privileged Identity Manager. *Security Intelligence*, 18.

ISACA. (2010). *Manual de Preparación al Examen CISA.* EE-UU: ISACA.

Jeremías. (2011). *Manual de auditoría de gestíon a las tecnologías de información y comunicaciones.* El Salvador: OLACEFs.

Matriz FODA. (15 de 8 de 2013). *http://www.matrizfoda.com/*. Obtenido de http://www.matrizfoda.com/

Organizations, C. o. (31 de Julio de 2014). *http://www.coso.org*. Obtenido de http://www.coso.org

Source, S. a. (27 de 08 de 2013). *http://auditorinformatico.blogspot.com/2012/09/historia.html*. Obtenido de http://auditorinformatico.blogspot.com/2012/09/historia.html

Tecniseguros. (2012). *Inventario de Software.* Quito: Tecnologia.

Tecniseguros. (13 de 08 de 2013). *http://www.tecniseguros.com.ec/trayectoria*. Obtenido de http://www.tecniseguros.com.ec/

Tecniseguros, C. D. (2009). *Plan Estrategico Empresarial.* Quito.