UNIVERSIDAD NACIONAL DE SANTIAGO DEL ESTERO
FACULTAD DE CIENCIAS EXACTAS Y TECNOLOGÍAS

LICENCIATURA EN SISTEMAS DE INFORMACIÓN

TRABAJO FINAL DE GRADUACIÓN

AUDITORÍA INFORMÁTICA UNA HERRAMIENTA PARA ENCAUZAR LA GOBERNABILIDAD DE LOS RECURSOS TECNOLÓGICOS DE INFORMACIÓN.

Autores:

AFTYKA CLAUDIA MARINA

ESPECHE HECTOR FABIAN

Profesor Guía**:**

LILIANA FIGUEROA

Agosto 2015

UNIVERSIDAD NACIONAL DE SANTIAGO DEL ESTERO

FACULTAD DE CIENCIAS EXACTAS Y TECNOLOGÍAS

TRABAJO FINAL DE GRADUACIÓN DE LA LICENCIATURA EN SISTEMAS DE INFORMACIÓN

AUDITORÍA INFORMÁTICA UNA HERRAMIENTA PARA ENCAUZAR LA GOBERNABILIDAD DE LOS RECURSOS TECNOLÓGICOS DE INFORMACIÓN.

Autor(es):

Aftyka Claudia Marina

Espeche Héctor Fabián

Profesor Guía:

Ing. Liliana Figueroa

————————————————————————————————————*

Aprobado el día ..... del mes de ..... del año 20..... por el Tribunal integrado por

....

....

Santiago del Estero – Argentina

DEDICATORIA

A dios

Por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional y personal.

A mis padres

Gracias viejo por estar siempre a mi lado apoyándome y aconsejándome, a pesar de nuestra distancia física, siento que estás conmigo, aunque nos faltaron muchas cosas por vivir juntos, como es, éste momento tan especial para mí. A mi madre por hacer de mí una mejor persona través de sus enseñanzas y de su gran amor.

A mis hermanos

Marcela, Eduardo, gracias por estar y acompañarme en cada proyecto de mi vida, a mi hermana Marisa, un agradecimiento especial, por ser un ejemplo de hermana mayor, por su constante preocupación y apoyo, a mi querido hermano Beto, que desde el cielo me ilumina el camino de la vida.

Los quiero mucho.

A mi amor Nelba

Gracias por todos estos años juntos, por haber compartido momentos hermosos y otros no tanto, pero siempre estuviste presente para brindarme tu apoyo constante, tu amor incondicional y alentarme a continuar cuando parecía que me rendía, por todo esto y por muchas cosas más, gracias por estar siempre a mi lado.

A Ceci

Mi hija del corazón, quien ha sido una motivación a no rendirme en los estudios y poder llegar a ser un ejemplo para ella.

A Marina

Mi compañera de Tesis, más que compañera una amiga, gracias por confiar en mí, por tu paciencia, tu dedicación; aprendimos a alentarnos y apoyarnos para poder superar los problemas que la vida nos presentaba, formando un gran equipo y poder llegar a este momento tan importante en nuestra formación profesional.

Héctor Fabián Espeche

DEDICATORIA

A mis padres

Pilares fundamentales de mi vida por darme el ejemplo de esfuerzo y sacrificio, brindarme su apoyo incondicional en cada momento de mi vida.

A Beto

Esposo y compañero, por su apoyo constante y amor incondicional. Te amo.

A Malena y Pilar

Mis hijas, que le dan sentido a mi vida.

A mis hermanos

Analia, Mara y Mariano, por darme la oportunidad de crecer al lado de ustedes y ser mejor día a día.

A mis sobrinos

Las dos Sofias, Renata y Lisandro, por su compañía, risas y travesuras.

A mis cuñados

Gabi, Maruco y Carlita, por estar siempre presentes.

A Fabián

Mi compañero de tesis, por brindarme su apoyo y amistad, por haber compartido solidaridad, dificultades y alegrías, durante todo el proceso de nuestro trabajo de tesis y superando obstáculos para alcanzar un objetivo en común. Gracias Fabi.

A mis amigos

Que siempre están apoyándome.

A la Academia

En las buenas y en las malas mucho más!!

Claudia Marina Aftyka

AGRADECIMIENTOS

A nuestra profesora guía Ing. Liliana Figueroa, gracias por su tiempo, por su apoyo como también por su sabiduría y conocimiento que nos transmitió en todo el desarrollo de nuestra tesis.

A todos nuestros compañeros y amigos que nos ayudaron y contribuyeron a lo largo de todo este trabajo académico, cada uno a su manera, escuchando, alentando, consolando, compartiendo alegrías, tristezas y conocimiento. Simplemente, gracias.

F.E. y M.A.

Santiago del Estero, Argentina

Mes de 2014

CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

Resumen

La misión de las Tecnologías de la Información (TI) es facilitar la consecución de los objetivos estratégicos de cualquier empresa. Para ello, se invierte en recursos humanos, equipos y tecnologías, además de los costos derivados de la posible organización estructural. Por lo tanto, esta inversión debe ser constantemente justificada en términos de eficacia y eficiencia.

En la actualidad empresarial, el desconocimiento de los beneficios de las TI, puede entenderse como un fenómeno organizacional caracterizado por el uso inapropiado de las mismas, que no solo implica graves perjuicios económicos, sino que afecta el ejercicio del negocio y por ende el grado de permanencia en el mercado.

En este contexto, surge el concepto de Gobierno de Tecnología de Información (GTI), definiéndolo como "Una estructura de relaciones y procesos para dirigir y controlar la empresa con el objeto de alcanzar sus objetivos organizacionales y añadir valor mientras se equilibran los riesgos y el retorno sobre TI." [1] El GTI permite a la empresa obtener ventajas competitivas tomando decisiones que le otorguen el crecimiento sostenido.

Al momento de la presentación de la propuesta de este trabajo, no se disponía de una metodología especifica de GTI sino marcos de trabajo que indican que hacer, pero no como. De acuerdo con los expertos, son buenas prácticas que deben ajustarse a las necesidades de cada organización, y deben aplicarse basándose en la experiencia y el sentido común. Además, las propuestas planteadas están orientadas a grandes organizaciones, caracterizadas por su formalidad; pocas son las propuestas que están orientadas a pequeñas organizaciones. Si bien existen algunas propuestas metodológicas están vinculadas con la gestión de recursos de TI, estas no son específicas para aplicar el concepto de GTI.

Para encaminar el GTI en una empresa, en este trabajo se propone una metodología para encaminar el GTI cuya herramienta principal es la Auditoría Informática (AI), la cual nos facilitará la revisión y evaluación de los controles, sistemas y procedimientos de informática, logrando con ello una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones de la empresa <2>. La AI está enmarcada por el estándar COBIT, el cual proporciona un conjunto de reglas de buenas prácticas para

el control de recursos de TI en una organización, las cuales tienen una aceptación internacional respaldada por ITGI (Instituto de Gobierno de TI).

Entendiendo a la AI como “el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficazmente los recursos”. [2] En este trabajo, se propone llevar a cabo una AI en el Área de TI de una empresa del medio basada en el estándar COBIT, lo cual permitirá que la empresa se encamine a la gobernabilidad de sus recursos de TI.

Introducción

Al predominar la idea de que las TI son consideradas como una función de apoyo y no como una función vital, sus posibilidades e impacto se ven limitadas. Esto conlleva a que su administración sea considerada más una cuestión técnica que una estrategia organizacional. Por lo tanto, las empresas necesitan manejar mejor la compleja tecnología que predomina en todas sus áreas y responder de forma rápida y segura a las necesidades del negocio; para ello deberán implementar una efectiva Gobernabilidad de TI con el fin de obtener los beneficios derivados de su uso.

El principal reto o dificultad de la implantación del GTI en empresas, tanto de nuestro medio como en general, es la falta de conocimiento sobre qué implica este tipo de estrategia y la falta concientización sobre la necesidad de contar con ella.

Un GTI conduce a la empresa a tomar total ventaja de su TI logrando con esto maximizar sus beneficios, capitalizar sus oportunidades y obtener ventaja competitiva.

El GTI permite vincular los procesos de TI, los recursos de TI y la información, con las estrategias y los objetivos de la empresa. Además, el GTI integra e institucionaliza buenas (o mejores) prácticas de gestión para asegurar que la información de la empresa y las tecnologías relacionadas den soporte a los objetivos del negocio.

Para poder alcanzar los objetivos del GTI resulta necesario certificar que las TI proporcionan la información que la empresa necesita para la toma de decisiones, esto se logra a través de una AI evaluando los controles necesarios para mitigar los riesgos tecnológicos para que los sistemas sean confiables y con un buen nivel de seguridad.

Si bien existen distintos estándares para llevar a cabo una AI, en esta propuesta se elige COBIT ya que es un estándar de aceptación y uso internacional, mediante el cual puede asegurar la integración entre el modelo de negocio, las estrategias de la empresa y las TI, estableciendo parámetros de administración, control y evaluación de cada uno de los procesos operativos y de administración de los recursos.

COBIT es un estándar de referencia para establecer controles sobre las TI y una guía de buenas prácticas para la gestión de la seguridad de los activos de información, y, sobre

todo, ayuda a las organizaciones a alcanzar sus objetivos, facilitando la comprensión y la gestión de los riesgos y del valor aportado por la información y sus tecnologías afines.

En este trabajo académico se desarrolla una propuesta metodológica del GTI para pequeñas y medianas empresas del medio que no disponen de una herramienta que permita organizar las actividades necesarias para poder encauzar la Gobernabilidad de sus recursos de TI. Cuando se hace referencia que la Metodología de Gobernabilidad de Recursos de TI encauza la Gobernabilidad, hacemos referencia a que dirige o guía a la empresa al alineamiento de las TI con las estrategias del negocio.

Esta metodología luego es adaptada a las características y necesidades de una empresa del medio.

Con el propósito de ayudar a encaminar a una empresa de nuestro medio hacia la gobernabilidad, se propone esta tesis que está compuesta por cuatro capítulos y un apartado dedicado a consideraciones finales.

El Capítulo I tiene como propósito delimitar y plantear el problema, para definir los objetivos y el alcance que se van a tener en cuenta en el desarrollo del presente trabajo.

El Capítulo II enuncia los marcos referenciales en los que se fundamenta el trabajo. El capítulo abarca tres secciones. En la sección II.1 se define el marco conceptual el cual se definen los conceptos sobre el cual se sustenta el trabajo que resulta de la investigación bibliográfica realizada. En la sección II.2 se especifica el marco metodológico, describiendo cada metodología utilizada en el trabajo académico. En la sección II.3 se describe el marco empírico en el cual se describe la empresa donde se aplica la solución propuesta.

En el Capítulo III se presenta una metodología que permite desarrollar el presente trabajo. Se muestran aspectos como la descripción de las fases de la metodología, las técnicas e instrumentos que fueron utilizados.

El Capítulo IV tiene como propósito aplicar la Metodología de Gobernabilidad en una empresa de nuestro medio.

Al final del trabajo académico se exponen conclusiones del trabajo académico.

CAPÍTULO I

PROBLEMA, OBJETIVOS Y ALCANCE

El propósito de este capítulo es delimitar y plantear el problema para definir los objetivos y el alcance que se van a tener en cuenta en el desarrollo del presente trabajo.

Es importante tener como objeto de estudio, el desempeño de las TI en la empresa, ya que muchas veces se la considera como una función de apoyo y no como una estrategia, es decir, que el recambio y la incorporación de las TI, se realiza sin tener en cuenta los riesgos asociados a ella y sin contar con un plan estratégico que nos brinde un mayor aprovechamiento de las TI.

I.1 PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

Un elemento crítico para el éxito y la supervivencia de las empresas, es la administración efectiva de la información y de la TI relacionada. [3]

Actualmente es imposible imaginar una empresa sin una dependencia en TI, no solo para manipular los datos operacionales, sino también para proveer la información de relevancia que la misma necesita.

Mientras muchas empresas están de acuerdo con los beneficios potenciales que les pueden brindar las TI, las empresas exitosas son las que logran entender y gestionar los riesgos asociados a la implementación de nuevas tecnologías <1>.

Si bien, el hardware y el software son accesibles por los competidores, hay que tener en cuenta que las TI por si solas no ayudan a crear ventajas competitivas estratégicas, lo que realmente es estratégico para una empresa, es la manera en que gestionan las TI y los riesgos a los que se ven afectados. Lograr esto es poder llevar a cabo la Gobernabilidad de las TI.

Las empresas de nuestro medio que han ido incorporando las TI sin una estrategia de gestión, han sufrido los siguientes inconvenientes:

- Los objetivos de los proyectos de Sistemas de Información no se encuentran alineados con los objetivos estratégicos de la empresa.
- No existe una gestión de los riesgos a los que se enfrentan.

- Existe una creciente vulnerabilidad de los Sistemas de Información.
- Los recursos no son usados responsablemente.

Una situación particular se presenta en una empresa de nuestro medio que comercializa seguros y tiene como principal activo la **información**, por lo tanto, su necesidad consiste en proteger este bien de todo tipo de riesgo que acarreé una pérdida de capital en la empresa. Es por ello, que la alta gerencia percibe el impacto significativo que la información tiene en el destino de la empresa. El potencial de las nuevas TI es tal, que puede llegar a introducir importantes cambios en la empresa y en las prácticas de su actividad, para crear nuevas oportunidades y reducir costos.

La ausencia de GTI en esta empresa trajo entre otros inconvenientes:

- Concepción de las TI como simple apoyo y no como función vital para el ciclo de crecimiento competitivo de la empresa.
- Inexistencia de metodologías y procesos de trabajo formales en el área informática.
- Pérdida de la información por fallos en los equipos, en los procesos o por una gestión inadecuada de los datos.
- Planes de adquisición de TI sin adecuados procesos de estudio, evaluación y beneficio para la empresa.
- Planes de capacitación en TI inoportunos.

En los últimos años, ante un ambiente cambiante y competitivo de la empresa de seguro, la alta gerencia ha incrementado sus expectativas relacionadas con sus recursos de TI, requiriendo niveles de servicio que representen incrementos en calidad, en funcionalidad y en facilidad de uso. Sin embargo, la alta gerencia percibe que las tomas de decisiones no se han visto modificadas considerablemente en el mayor aprovechamiento de su principal activo, la información, a pesar de las inversiones realizadas en los recursos de TI.

La necesidad de la empresa de seguro consiste en salvaguardar la información de todo tipo de riesgo o una mala manipulación que acarreé una pérdida de capital en la empresa. Es por ello, que cada vez más la alta gerencia percibe el impacto significativo que la información tiene en el destino de la empresa. El potencial de las nuevas TI es tal, que puede llegar a introducir importantes cambios en la empresa y en las prácticas de su actividad, para crear nuevas oportunidades y reducir costos.

Ante la necesidad prioritaria de la empresa de seguro, de garantizar la seguridad de la información, se llevará a cabo una AI la cual evaluará los controles necesarios para otorgar una garantía razonable de la integridad, confiabilidad y disponibilidad de la información empresarial. En base a los resultados de la AI, se establecerán las recomendaciones necesarias para encauzarla Gobernabilidad de los recursos tecnológicos, y así, apoyar los objetivos del negocio de forma correcta y en los tiempos precisos.

I.2 ANTECEDENTES

La AI basada en el estándar COBIT ha sido aceptada por muchas organizaciones en el ámbito global y se continúan documentando nuevos casos.

A nivel internacional, existen casos de estudio en que describen la implementación de COBIT en sus empresas:

- CASO 1: John Beveridge, CISA oficina del auditor del estado de Massachusetts Estados Unidos, señala: "Nuestra experiencia con COBIT también ha ayudado a los auditores poco experimentados a comprender los procesos de TI y los objetivos detallados de control, y para delimitar esto dentro de la organización auditada y el ambiente de TI. Mediante la implantación de COBIT, hemos identificado la necesidad de mejorar y enmendar lineamientos de auditoría genéricos, manuales de procedimientos de auditoría y revisiones de aseguramiento de calidad."<4>
- CASO 2: PRATAP OAK, auditor senior de TI Jay Stott, vicepresidente, auditoría de TI fidelity investments boston, Massachusetts, Estados Unidos de América, señala: "Mediante la implantación de COBIT, hemos incorporado en nuestras auditorías un cuerpo de conocimientos completo sobre los controles. COBIT proporciona una base experta de los controles de TI y ayuda a asegurar una cobertura completa, eficiente y consistente del ambiente de control de TI. En el futuro, planeamos utilizar COBIT para controlar las revisiones de auto – evaluación y para reforzar el ambiente de control. Proporciona una base para medir mejor el estado del ambiente de control de TI y es lo suficientemente flexible para apoyar nuestros objetivos a través de muchos cambios por venir."<4>
- CASO 3: UPS. United Postal Services, es una de las más grandes empresas de mensajería del mundo. En 1986 UPS se veía perdiendo terreno ante FedEx y su posibilidad de rastreo de paquetes. Una inversión de más de $11 mil millones en un

lapso de 10 años en centros de datos, expertos tecnológicos, creación de una red global, bases de datos y aplicaciones integradas. Sin embargo, UPS no invirtió únicamente dinero, invirtió esfuerzo de la directiva y esfuerzo en definir el escenario claro para la alineación estratégica de las inversiones de TI con los objetivos del negocio, de esta manera generando mayor valor y beneficios e implementando procesos de GTI que habiliten y aseguren decisiones de TI efectivas. Las raíces del sistema de GTI implementado en UPS se encuentran en un Comité de Dirección que define el rol de las TI en la organización y una clara dirección tecnológica. En la búsqueda de una organización de TI totalmente alineada con la estrategia de negocio, UPS tomó la decisión de crear un Comité de GTI para controlar las operaciones de TI día a día, manejar procesos de priorización de proyectos y de aprobación de presupuestos, estándares de TI, y la creación de políticas para normar las operaciones.<4>

- CASO 4: CANADIAN TIRE FINANCIAL SERVICES (CTFS) es una empresa que trabaja desde 1961 y actualmente presta servicios financieros a más de 3 millones de clientes a través de su tarjeta “Canadian Tire Options Mastercard®” con más de 1700 empleados. La necesidad de implementar un sistema de GTI surge por requerimientos de certificación CEO/CFO canadiense. Para poder implementar exitosamente un GTI y alcanzar los requerimientos de la certificación CEO/CFO se recomendó la utilización de COBIT como herramienta principal por el reconocimiento internacional y por su facilidad de medición de cumplimiento de controles internos<5>. Una vez implementado COBIT en CTFS se logró lo siguiente:

  - Facilidad de creación de planes de trabajo de la auditoría interna de tecnologías de información. Basándose en las áreas de proceso y entregando resultados escalables.
  - La herramienta fue utilizada para evaluar el riesgo de TI basándose en objetivos de control establecidos y procesos de evaluación de riesgo.
  - Capacidad de analizar y evaluar áreas críticas del negocio, sus sistemas y aplicaciones asociadas a cada una de las unidades del negocio.
  - Entregar a administradores, auditores y usuarios un sistema de métricas e indicadores claves para medir el desempeño de las TI.

La implementación de un sistema de GTI basado en los procesos de COBIT permitió a CTFS tener un nivel de respuesta muy aceptable para los requerimientos y retos de la certificación anual de CEO/CFO.

A nivel nacional y local, el estándar COBIT es nuevo, y por sus antecedentes, recién hoy las empresas consultoras la están teniendo en cuenta para realizar las AI. Según un informe presentado por ISACA sobre la incorporación de COBIT en los organismos gubernamentales y de regulación en América latina, en octubre de 2003, registros en Argentina señalan<12>:

- El Banco Central ha seleccionado COBIT como la base de normas y procedimientos para todas las instituciones financieras. Además, COBIT también ha sido utilizado para definir los objetivos de control para los locales de centros de intercambio de información que son fiscalizados por el Banco Central.
- En la provincia de Mendoza, COBIT ha sido adoptado por ley y es el marco que se utiliza en la actualidad por el Tribunal de Cuentas en su proyecto de implementar el GTI.
- La Sindicatura General de la Nación y la Auditoría General de la Nación, que son órganos de control de Auditoría y presentación de informes al Poder Ejecutivo y el Congreso, respectivamente, también han adoptado COBIT.

Con respecto a la implementación del GTI en Argentina, son pocas las empresas que gestionan sus TI, son solo iniciativas aisladas o corporativas que bajan línea desde la casa matriz. Por lo tanto, se deduce que las TI no se usan, en general, de una manera que contribuya a la generación de valor agregado. Para cambiar esta situación, es imprescindible eliminar los métodos rudimentarios en los negocios de todos los sectores, con bajo uso de TI orientadas a la gestión, en comparación a las mejores prácticas conocidas en el mundo. En relación a lo anterior, es evidente que para generar productividad no sólo hay que tener las TI, sino hay que darles un adecuado uso, teniendo buenas políticas de gestión, que le saquen el mejor partido. [11]

I.3 JUSTIFICACIÓN

La dependencia de las empresas en TI ha crecido a tal punto que una interrupción prolongada en las operaciones de los sistemas de información puede suspender la continuidad de sus operaciones.

De esta manera, las TI se han convertido en uno de los factores claves de contribución para que las empresas puedan alcanzar sus objetivos de negocio. Sin embargo, el desconocimiento de muchas empresas sobre los beneficios de las TI han llevado a que ésta, sea más un inhibidor que un catalizador del rendimiento empresarial.

Hasta hace poco tiempo, era una práctica común considerar el Área de TI de una organización como algo separado y diferenciado del resto del negocio. En la actualidad, las funciones de TI están presentes en todas las áreas, debido a la dependencia de la información y de las TI asociadas, para respaldar los procesos de negocio más relevantes.

A esta realidad no se encuentra ajena las empresas de nuestro medio y en particular la empresa seguro, en donde las distintas áreas operativas se sostienen y apoyan cada vez más en los servicios de las TI que han acompañado la automatización y el crecimiento de todos los procesos y la prestación de nuevos servicios. Como consecuencia, la información y la tecnología que la soporta representan un activo valioso, ya que su productividad depende del funcionamiento ininterrumpido de los sistemas, transformando a todo el entorno como un proceso crítico adicional. Ahora, bajo el concepto de GTI, se buscará gestionar las TI de una manera estratégica, para establecer explícitamente cuáles decisiones deben tomarse alrededor de las TI y quien debe tomarlas.

Para encauzar el GTI primero se debe tener un panorama real de la empresa de seguro en la gestión de las TI, para ello se llevará a cabo una AI que tiene como función evaluar controles y procedimientos establecidos por la empresa en todo lo relacionado con la información y las TI, de manera de minimizar los riesgos que amenacen la efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información [6].

El uso del estándar COBIT en la AI, motiva el desarrollo de políticas claras y buenas prácticas para el control de TI de toda la empresa. Por lo tanto, COBIT está orientado a ser la herramienta de GTI que ayude al entendimiento y a la administración de riesgos asociados con las TI y con tecnologías relacionadas. [1]

Para satisfacer los objetivos del negocio, es necesario que la información este de acuerdo a los criterios que COBIT define como requerimientos de negocio para la información. Estos son:

- Requerimientos de Calidad: Calidad, Costo, Entrega o Distribución (de servicio)
- Requerimientos Fiduciarios: Efectividad y Eficiencia de las Operaciones, Confiabilidad de la Información y Cumplimiento de las Leyes y Regulaciones.
- Requerimientos de Seguridad: Confidencialidad, Integridad y Disponibilidad.

Considerando que la información constituye el activo más importante para la empresa de seguro, el principal problema que debe resolverse es la protección permanente de su información crítica que actualmente se ve afectada por factores tales como, una débil estructura de perfiles de usuario, falla de disco, ataques de códigos maliciosos, y otros. Es por ello, que se considera que el requerimiento de seguridad de información es la prioridad de la empresa bajo estudio.

El objetivo del presente trabajo, es encaminar la gobernabilidad del Área de TI, realizando una AI con el apoyo del estándar COBIT, evaluando los recursos de TI e institucionalizando las buenas prácticas para asegurar los objetivos estratégicos de la empresa.

I.4 OBJETIVOS

I.4.1 Objetivo general:

Realizar una AI al Área de TI de una empresa de seguro, que evalúe los controles de la seguridad de la información, y realizar las recomendaciones pertinentes para encauzar la gobernabilidad de este requerimiento de negocio.

I.4.2 Objetivo específicos:

- Seleccionar los procesos de TI que garantizan la seguridad de la información.
- Establecer el estado de madurez de los procesos de TI relacionados a la seguridad de la información.
- Elaborar un plan de AI a ser implementado en la empresa seleccionada como caso de estudio.
- Auditar los procesos de TI seleccionados, aplicando el estándar COBIT.
- Realizar las recomendaciones necesarias en base a los resultados obtenidos en la AI.

I.5 ALCANCE

Se selecciona el Área de TI de la empresa de seguro como caso de estudio que posibilite la puesta en práctica de la propuesta de trabajo.

Esta Área se selecciona por considerarla critica, teniendo en cuenta que los errores o las deficiencias de esta, tienen un impacto directo para la empresa, ya sea económico, de eficiencia y de cumplimiento legal normativo.

Luego de la selección del área, se recurre a la AI para revisar y evaluar los controles de los procesos de TI.

Para definir el alcance de la AI en el Área de TI, se tienen en cuenta los requerimientos de negocio definidos por COBIT, seleccionando el de seguridad de la información ante la necesidad de la empresa de seguro de salvaguardar este recurso que constituye el principal activo del funcionamiento operativo de la misma.

A partir de la AI, que permite disponer de la evaluación de los controles y procedimientos de la empresa, se plantean las mejoras necesarias para encaminar el GTI al Área de TI de la empresa de seguro, teniendo en cuenta el requerimiento de negocio definido por COBIT, seguridad de la información.

CAPÍTULO II

MARCOS REFERENCIALES

El presente capítulo enuncia los marcos referenciales en los que se fundamenta el trabajo.

El capítulo abarca tres secciones. En la sección II.1 se define el marco conceptual el cual ayuda a decidir y a explicar el camino seleccionado en la resolución del problema. En la sección II.2 se especifica el marco metodológico, describiendo cada metodología utilizada en el trabajo académico. En la sección II.3 se describe el marco empírico en el cual se presenta la empresa donde se aplica la solución propuesta.

II.1 MARCO CONCEPTUAL

El marco conceptual es la etapa del proceso de investigación en que se establece la teoría que ordena la investigación, es decir, la teoría que se está siguiendo como modelo de la realidad que se está investigando, esto permitirá unificar criterios sobre el significado de los términos y justificar porque se lleva a cabo este trabajo de una manera determinada.

II.1.1Información <10>

En sentido general, la información es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Según otro punto de vista, la información es un fenómeno que proporciona significado o sentido a las cosas, e indica mediante códigos y conjuntos de datos, los modelos del pensamiento humano. La información por tanto, procesa y genera el conocimiento humano. Aunque muchos seres vivos se comunican transmitiendo información para su supervivencia, la diferencia de los seres humanos radica en su capacidad de generar y perfeccionar tanto códigos como símbolos con significados que conformaron lenguajes comunes útiles para la convivencia en sociedad, a partir del establecimiento de sistemas de señales y lenguajes para la comunicación. <10>

II.1.2 Seguridad de la Información [13]

Se entiende por **Seguridad de la Información** a todas aquellas medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información, buscando mantenerla confiable, disponible e integra.

El objetivo de la seguridad de la información, que circula por las redes o esta almacenada en los sistemas informáticos, es doble:

- Mantener el secreto, evitando los accesos no autorizados.
- Mantener la autenticidad evitando modificaciones no autorizadas.

Las diversas técnicas de seguridad se desarrollaron con la aparición de los primeros ataque a la información por parte de intrusos interesados en el contenido de éstas. Los tipos de ataques en contra de los sistemas de seguridad informáticos o una red de datos pueden ser muy diversos y provenir de distintas fuentes (Ver Figura II.1 Ataques a Sistemas Informáticos); por todo ello, las técnicas que se empleen para protegerlos han de ser muy variadas y tener en cuenta todos los aspectos particulares que se pueden dar, para que sean efectivas.

Figura II.1 Ataques a Sistemas Informáticos

En general en una comunicación hay un flujo de información desde una fuente hacia un destino remoto, que está expuesta a cuatro categorías generales de ataque: Interrupción, Intercepción, Modificación y Generación (Ver Figura II.2 Ejemplos de Ataques al Sistema Informático).

- **Interrupción**. La información del sistema es destruida o llega a ser inutilizable. Este es un ataque sobre la disponibilidad. Ejemplo de este tipo de ataque son la destrucción de un disco duro o el corte de una línea de comunicación.
- **Interceptación**. Una participación sin autorización por parte de una persona, ordenador o programa en una comunicación. Este es un ataque sobre la confidencialidad. Un ejemplo de ataque podría ser la copia ilegal de programas o archivos.
- **Modificación**. Una participación sin autorización, pero no sólo accedió a la información si no también alterándola. Este es un ataque sobre la integridad. Ejemplos

podrían ser los cambios de valores en archivos y programas o la modificación de mensajes transmitidos en una red.

- **Generación**. Introducción de objetos falsificados en un sistema sin autorización. Este es un ataque sobre la autenticidad. Un ejemplo sería la introducción de mensajes falsos en una red.

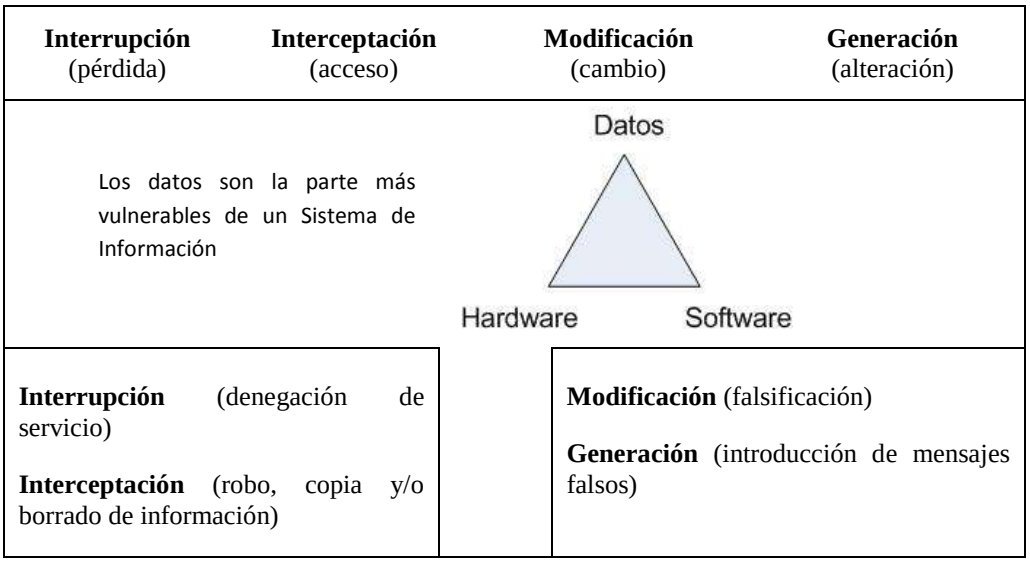


Figura II.2 Ejemplos de Ataques al Sistema Informático

Estos tipos de ataque se pueden incluir en dos categorías de ataques, los pasivos y los activos:

- **Ataque pasivo**: los ataque pasivos son, simplemente, observaciones de datos reservados durante una transmisión. La finalidad del intruso es la obtención de la información transmitida. Dentro de ellos nos encontramos dos tipos de ataque: observación del contenido del ataque y el análisis de tráfico.

    - El primero sería el entendimiento por parte de un intruso del contenido de una transmisión que contiene información confidencial, como una conversación telefónica o correo electrónico.

    - El análisis de tráfico seria la observación, por parte del intruso, sobre la longitud del mensaje, la identificación de los usuarios y la frecuencia de transmisión, pero en ningún caso puede entender la información, pues va encriptada. Los ataques pasivos, son difícilmente detectables, porque no producen una alteración de la información; no obstante, son factibles de prevenir.

- **Ataque activos**: los ataques activos incluyen alguna modificación del mensaje o la creación de mensajes falsos. Hay varios tipos de ataques activos:

    - **Cambiar la identidad del emisor o receptor**: Ocurre cuando una entidad pretende hacerse pasar por otra.

    - **Manipulación de datos**: La información se ve alterada, sustituyendo la original por otra con el fin de engañar al receptor.

    - **Repetición**: Capturar una información, guardarla un tiempo y volverla a enviar, produciendo un efecto de no autorización.

    - **Denegación de servicios**: Impedir una comunicación con un centro servidor, obtener una respuesta o causar un repudio de usuario.

Los hackers y curiosos (persona que simplemente curiosean en el sistema, por ejemplo, para leer el correo de alguien) protagonizan la mayoría de los ataques en las redes. Por otra parte, los crackers, suelen aprovechar las debilidades de estas redes para realizar sus travesuras o simplemente, para utilizar los equipos como intermediarios a su verdadero blanco.

Pero el mayor porcentaje de los ataques que se producen en las empresas lo realizan ex empleados descontentos con las mismas. La peligrosidad de estas personas así como el alcance de los ataques es muy alta, ya que conocen a la perfección el sistema.

El robo de información, realizado por miembros de la propia organización, o por personas que saben de su existencia está, por desgracia, a la orden del día.

La interceptación de las comunicaciones, hasta las sustracción de portátiles, CD, móviles, y otros dispositivos, ponen en peligro tanto la confidencialidad de los datos como las fragilidad de nuestras estrategias, si son conocidas a destiempo fuera de la organización. El valor que tiene la información para la competencia, así como la responsabilidad que esta tiene sobre los datos de tercero que contempla la normativa de protección de datos, ponen de manifiesto el riesgo real de que existe fuga de información sensible, a la que se debe ampliar una mayor protección, haciendo inaccesible la información situada tanto en soportes físicos, como en la red y las comunicaciones si los usuarios no están correctamente autenticados.

En el extremo de la peligrosidad están los intrusos remunerados, o sea, personas a las que una tercera persona les paga para que realicen un "trabajo". Afortunadamente son los menos comunes, pero son personas con amplia experiencia en el campo de la seguridad y con profundo conocimiento de sistemas informáticos.

II.1.2.1 Seguridad y el Control en las Organizaciones [14]

Muchas empresas se muestran reacias a invertir demasiado en seguridad porque no está directamente relacionada con los ingresos por las ventas. Sin embargo la protección de los Sistemas de Información es tan crucial para el funcionamiento del negocio que merece un análisis.

Las empresas tienen activos de información muy valiosos que deben proteger. Con frecuencia los sistemas albergan información confidencial sobre los impuestos, activos financieros, registros médicos y revisiones del desempeño laboral de los empleados. También contienen información acerca de las operaciones corporativas incluyendo secretos comerciales, planes de desarrollo de nuevos productos y estrategias de marketing. Los sistemas gubernamentales podrían almacenar información sobre sistemas de armas, operaciones de inteligencia y objetivos militares. Estos activos de información tienen un valor enorme y si se perdieran, destruyeran o cayeran en manos equivocadas podrían tener repercusiones desbastadoras.

La seguridad y el control inadecuados también pueden dar lugar a serios problemas de responsabilidad legal. Las empresas deben proteger no solo sus propios activos de información, sino también los de sus clientes, empleados y socios de negocios. En caso contrario, la empresa podría verse involucrada en costosos litigios por exposición o robo de datos. Una empresa puede ser responsabilizada por daños innecesarios si no toma las medidas de protección para prevenir la pérdida de información confidencial, la alteración de datos o la violación de la privacidad. En consecuencia, una sólida estructura de seguridad y control que proteja los activos de información del negocio pueden generar un alto rendimiento de la inversión.

II.1.2.2 Mecanismos de Seguridad

Para proteger al sistema, consideremos las amenazas potenciales que pueden comprometerlo así como también la probabilidad de ocurrencia. A partir de esto, tendremos que definir una política de seguridad que divida responsabilidades y establezca

reglas a seguir para evitar las amenazas o para minimizar sus efectos en el caso de que ocurra. A los mecanismos utilizados para implementar la política de seguridad se les denomina "mecanismos de seguridad". Estos mecanismos se dividen en tres grandes grupos:**[**13]

- **Mecanismos de Prevención:** Son aquellos que tratan de evitar la ocurrencia de violaciones de seguridad. Por ejemplo, el cifrado de las comunicaciones o la instalación de programas antidialers, son mecanismos de prevención.

- **Mecanismos de Detección:** Detentan las violaciones o intentos de violación del sistema en el momento de producirse (o cuando se ha intentado y no se ha conseguido) dentro de este tipo mecanismo tenemos las herramientas de auditorías.

- **Mecanismo de Recuperación:** Se aplican cuando la violación del sistema ya se ha producido, y trata de devolver a éste a un estado correcto de funcionamiento. Podemos citar como ejemplo las copias de seguridad.

  Dentro de este grupo se engloban también los mecanismos de análisis forense, cuyo objetivo no es solo el citado para los mecanismos de recuperación si no también averiguar el alcance de la violación y conocer los mecanismos que ha utilizado el intruso para comprometer el sistema, de modo que se prevengan otros ataque similares a la red.

Evidentemente detectar un ataque en el momento en que se produce (o mejor aún antes de que se produzca) es mucho más productivo y menos comprometedor para el sistema que el tener que recuperarlo mediante copia de seguridad. (Ver Figura II.3 Mecanismos de Seguridad)

Figura II.3 Mecanismo de Seguridad

II.1.2.3 Políticas de Seguridad [13]

Todas las empresas deberían tener protegida su información mediante diversas técnicas de seguridad. A la descripción, bajo la forma de reglas, en la que se incluyen propiedades de integridad, confiabilidad y disponibilidad, en la medida requerida por la empresa, se la conoce como Política de Seguridad.

El objetivo de las políticas de seguridad es definir que están haciendo los usuarios con la información de la empresa, para hacer un buen uso de los recursos de hardware y software y, por supuesto, tener eficacia en los costos.

Cada uno de los procesos administrativos o técnicos que se manejen en los SI debería contar con su propia política de seguridad y los atributos descriptos a continuación deberán ser aplicados al definir estas.

Para la seguridad de la información se cuenta con los siguientes atributos:

- **Confiabilidad**: Se refiere a tener la información restringida a aquellos sujetos que no tienen autorización; solamente usuarios definidos por la dirección de la empresa tendrán acceso a la información.
- **Integridad**: Para la empresa es muy importante que su información se mantenga sin modificación y que los sujetos que están autorizados para hacerlo trabajen bajo estrictas normas de operación.
- **Disponibilidad**: Es muy importante que la información de los sistemas esté disponible en cualquier momento que lo necesiten los usuarios designados o procesos autorizados.

II.1.3 Auditoría [9]

El concepto de Auditoría es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una sección, un organismo, una entidad, etc.

Conceptualmente la auditoría, "es la actividad consistente en la emisión de una opinión profesional sobre si el objetivo sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescriptas".

Podemos descomponer este concepto en los elementos fundamentales que a continuación se especifican:

- Contenido: una opinión.
- Condiciones: profesional
- Justificación: sustentada en determinados procedimientos
- Objetivo: una determinada información obtenida en un cierto soporte
- Finalidad: determinar si presenta adecuadamente la realidad o ésta responde a la expectativa que le son atribuidas, es decir, su finalidad.

En todo caso es una función que se ejecuta a posteriori, en relación con actividades ya realizadas, sobre las que hay que emitir una opinión.

II.1.3.1 Tipos de Auditoría [9]

Los elementos objetivos y finalidad, nombrados en el apartado anterior, distinguen de qué tipo de auditoría se trata. El objeto sometido a estudio, sea cual sea su soporte, por una parte, y la finalidad con que se realiza el estudio, define el tipo de auditoría de que se trata. En la Tabla II.1 Tipos de Auditoría, se muestra una clasificación de los tipos de auditoría.

Tabla II.1 Tipos de Auditoría

Tipos	Objeto	Finalidad
Financiera	Cuentas anuales	Presentan la realidad financiera de la empresa.
Informática	Sistemas Informáticos, recursos informáticos, planes de contingencia y aplicaciones informáticas.	Operatividad eficiente, según normas establecidas.
Gestión	Dirección	Eficacia, eficiencia, economicidad.
Cumplimiento	Normas establecidas.	Las operaciones se adecuan a estas normas.

II.1.3.2 Auditoría Informática (AI) [6]

La Informática está dentro de la gestión integral de la empresa, y por eso, las normas y estándares propiamente informáticos deben estar, sometidos a los generales de la misma. Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, desde el momento en que es una herramienta adecuada de colaboración. En este sentido y debido a su importancia en el funcionamiento de una empresa, existe la AI.

La AI se la puede definir como:

- Según el autor Rivas es: *"el conjunto de técnicas, actividades y procedimientos, destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control, eficacia, seguridad y adecuación de los Sistema de Información en la empresa".*
- Según el ISACA AI es: *"el proceso de revisión y evaluación, parcial o completo de los aspectos relacionados con el procesamiento automatizado de la Información".*

La función de la AI es garantizar el cumplimiento de las normas y procedimientos establecidos por la empresa en todo lo relacionado con la información y la TI, de manera de minimizar los riesgos que amenacen la efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información. [6]

Los principales objetivos que constituyen a la AI son el control de la función informática, el análisis de la eficiencia de los SI que comporta, la verificación del cumplimiento de la normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos informáticos. <9>

La AI es fundamental para garantizar el correcto funcionamiento de los Sistemas de Información al proporcionar los controles necesarios que permiten garantizar la seguridad, integridad, disponibilidad y confiabilidad de los mismos. [2]

El auditor evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informativos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso del software. En muchos casos ya no es posible verificar manualmente los procedimientos informatizados que resumen, calculan y clasifican datos, por lo que se deberá emplear software de auditoría y otras técnicas asistidas por computadora.

El auditor es responsable de revisar e informar a la Dirección de la Organización sobre el diseño y el funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada.

Se puede establecer tres grupos de funciones a realizar por un auditor informático [9]:

- Participar en las revisiones durante y después del diseño, realización, implantación y explotación de aplicaciones informáticas, así como en las fases análogas de cambios importantes.

- Revisar y juzgar los controles implantados en los sistemas informáticos para verificar su adecuación a las órdenes e instrucciones de la Dirección, requisitos legales, protección e confidencialidad y cobertura entre errores y fraudes.

- Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos e información.

II.1.4 Control Interno Informático [9]

El Control Interno Informático controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijadas por la Dirección de la Organización y/o la Dirección de Informática, así como los requerimientos legales.

La misión de Control Interno Informático es asegurar que las medidas que se obtienen de los mecanismos implantados por cada responsable son correctas y válidas.

El Control Interno Informático suele estar a cargo de un órgano staff dotado de las personas y medios materiales necesarios para las obligaciones que se les encomienda.

Como principales objetivos podemos indicar los siguientes:

- Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijadas, evaluar su bondad y asegurar del cumplimiento de las normas legales.
- Asesorar sobre el cumplimiento de las normas.
- Colaborar y apoyar el trabajo de AI, así como de la auditoría externa.
- Definir, implementar y ejecutar mecanismos y controles para comprobar el logro de los niveles del servicio informático, lo cual no debe considerarse como que la implementación de los mecanismos de medida y la responsabilidad del logro de esos niveles se ubique exclusivamente en la función de Control Interno, sino que

cada responsable de objetivos y recursos es responsable de esos niveles, así como de la implementación de los medios de medida adecuados.

Realizar el control de las diferentes actividades operativas sobre:

- El cumplimiento de procedimientos, normas y controles dictados. Merece resaltarse la vigilancia sobre el control de cambio y versiones del software.
- La producción diaria.
- La calidad y eficiencia del desarrollo y mantenimiento del software y del servicio informático.
- Las redes de comunicaciones.
- El software de base.
- Los sistemas microinformáticos.
- La seguridad informática (su responsabilidad puede estar asignada a control interno o bien puede asignársele la responsabilidad de control dual de la misma cuando está encargada a otro órgano):
  - Usuario, responsables y perfiles de uso de archivos y base de datos.
  - Normas de seguridad.
  - Control de información clasificada.
  - Control dual de la seguridad informática.
- Licencias y relaciones contractuales con terceros.
- Asesorar y transmitir cultura sobre el riesgo informático.

II.1.4.1 Sistema de Control Interno Informático [9]

Se puede definir el control interno como "cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar el funcionamiento de un sistema para conseguir sus objetivos".

Los controles cuando se diseñen, desarrollen e implanten han de ser al menos completos, simples, fiables, revisables, adecuados y rentables. Respecto a esto último habrá que analizar la evaluación costo-riesgo y el riesgo de su implementación.

Los controles internos que se utilizan en el entorno informático continúan evolucionando hoy en día a medida que los sistemas informáticos se vuelven complejos. Los progresos que se producen en la tecnología de soportes físicos y de software han modificado de manera significativa los procedimientos que se empleaban tradicionalmente para controlar los procesos de aplicaciones y para gestionar los Sistemas de Información.

Para asegurar la integridad, disponibilidad y eficacia de los sistemas se requieren complejos mecanismos de control, la mayoría de los cuales son automáticos. Resulta interesante observar, sin embargo, que hasta en los sistemas cliente/servidor avanzados, algunos controles son completamente automáticos, otros son completamente manuales y muchos dependen de una combinación de elementos de software y de procedimientos.

Históricamente los objetivos de los controles informáticos se han clasificado en las siguientes categorías:

- **Controles preventivos**: para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.
- **Controles detectivos:** cuando fallan los preventivos para tratar de conocer cuanto antes el evento. Por ejemplo, el registro de intentos de acceso no autorizados, el registro de la actividad diaria para detectar errores u omisiones, etc.
- **Controles correctivos**: facilitan la vuelta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un archivo dañado a partir de las copias de seguridad.

Como el concepto de controles se originó en la auditoría, resulta importante conocer la relación que existe entre los métodos de control, los objetivos de control y los objetivos de auditoría. Se trata de un tema difícil por el hecho de que, históricamente, cada método de control ha estado asociado unívocamente con un objetivo de control (por ejemplo, la seguridad de archivos de datos se conseguía sencillamente controlando el acceso).

Sin embargo, a medida de que los sistemas informáticos se han vuelto más complejos, los controles informáticos han evolucionado hasta convertirse en procesos integrados en los que se atenúan las diferencias entre las categorías tradiciones de controles informáticos.

Por ejemplo, en los actuales sistemas informáticos puede resultar difícil ver la diferencia entre seguridad de los programas, de los datos y objetivos de control del software del sistema, porque el mismo grupo de métodos de control satisface casi totalmente los tres objetivos de control.

La relación que existe entre los métodos de control y los objetivos de control puede demostrarse mediante el siguiente ejemplo, en el que un mismo conjunto de métodos de control se utiliza para satisfacer objetivos de control tanto de mantenimiento como de seguridad de los programas:

- **Objetivo de control de mantenimiento**: asegurar que las modificaciones de los procedimientos programados está adecuadamente diseñadas, probadas, aprobadas e implantadas.
- **Objetivo de control de seguridad de programas**: garantizar que no se pueden efectuar cambios no autorizados en los procedimientos programados.

II.1.4.2 Implementación de un Sistema de Controles Internos Informáticos [9]

Los controles pueden implementarse a varios niveles diferentes. La evaluación de los controles de la TI exige analizar diversos elementos interdependientes. Por ello es importante llegar a conocer bien la configuración del sistema, con el objeto de identificar los elementos, productos y herramientas que existen para saber dónde pueden implantarse los controles, así como para identificar posibles riesgos.

Para llegar a conocer la configuración del sistema es necesario documentar los detalles de:

- **Entorno de red**: esquema de la red, descripción de la configuración hardware de comunicaciones, descripción del software que se utiliza como acceso a las telecomunicaciones, control de red, situación general de los computadores de entornos de base que soportan aplicaciones críticas y consideraciones relativas a la seguridad de la red.
- **Configuración del computador base**: configuración del soporte físico, entorno del sistema operativo, software con particiones, entornos (pruebas y real), bibliotecas de programas y conjunto de datos.
- **Entorno de aplicaciones:** procesos de transacciones, sistemas de gestión de base de datos y entornos de procesos distribuidos.
- **Productos y herramientas**: software para desarrollo de aplicaciones, software de gestión de bibliotecas, integridad del sistema, controles de supervisión, etc.
- **Seguridad del computador base**: identificar y verificar usuarios, control de acceso, registro e información, integridad del sistema, controles de supervisión, etc.

Para la implementación de un sistema de controles internos informáticos habrá que definir políticas, pautas y normas técnicas que sirvan de base para el diseño y la implementación de los Sistemas de Información y de los controles correspondientes. Entre ellos:

- **Administración de sistemas**: controles sobre la actividad de los centros de datos y otras funciones de apoyo al sistema, incluyendo la administración de las redes.

- **Seguridad:** incluye las tres clases de controles fundamentales implantados en el software del sistema, integridad del sistema, confidencialidad (control de acceso) y disponibilidad.

- **Gestión del cambio:** separación de las pruebas y la producción a nivel de software y controles de procedimientos para la migración de programas software aprobados y probados.

La implantación de una política y cultura sobre la seguridad requiere que sea realizada por fases y esté respaldada por la Dirección. (Ver Figura II.4 Implementación de Política y Cultura Sobre Seguridad)

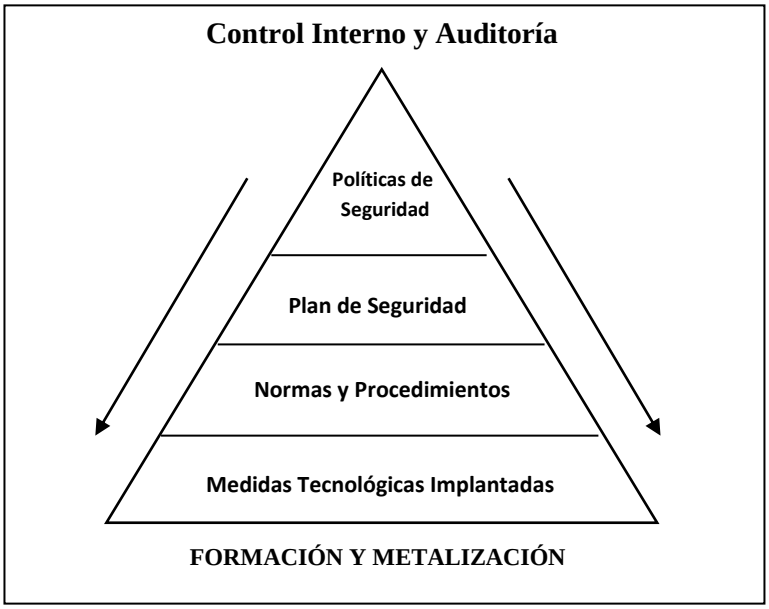


Figura II.4 Implementación de Política y Cultura Sobre Seguridad

Cada función juega un papel importante en las distintas etapas:

- **Dirección de Negocio o Dirección de Sistema de Información:** define la política y/o directrices para los Sistemas de Información en base a las exigencias del negocio, que podrán ser internas o externas.
- **Dirección de Informática:** define las normas de funcionamiento del entorno informático y de cada una de las funciones de informática mediante la creación y publicación de procedimientos, estándares, metodología y normas aplicables a

todas las áreas de informática así como a los usuarios, que establezcan el marco de funcionamiento.

- **Control Interno Informático:** define los diferentes controles periódicos a realizar en cada una de las funciones informáticas, de acuerdo al nivel de riesgo de cada una de ellas y ser diseñados conforme a los objetivos del negocio y dentro del marco legal aplicable. Estos se plasmarán en los oportunos procedimientos de control interno y podrán ser preventivos o de detección. Realizará periódicamente la revisión de los controles internos informáticos establecidos informando de las desviaciones a la Dirección de Informática y sugiriendo cambios que crea conveniente en los controles, así como también transmitirá constantemente a toda la organización la cultura y políticas del riesgo informático. (Ver Figura II.5 Funcionamiento del Control Interno Informático)

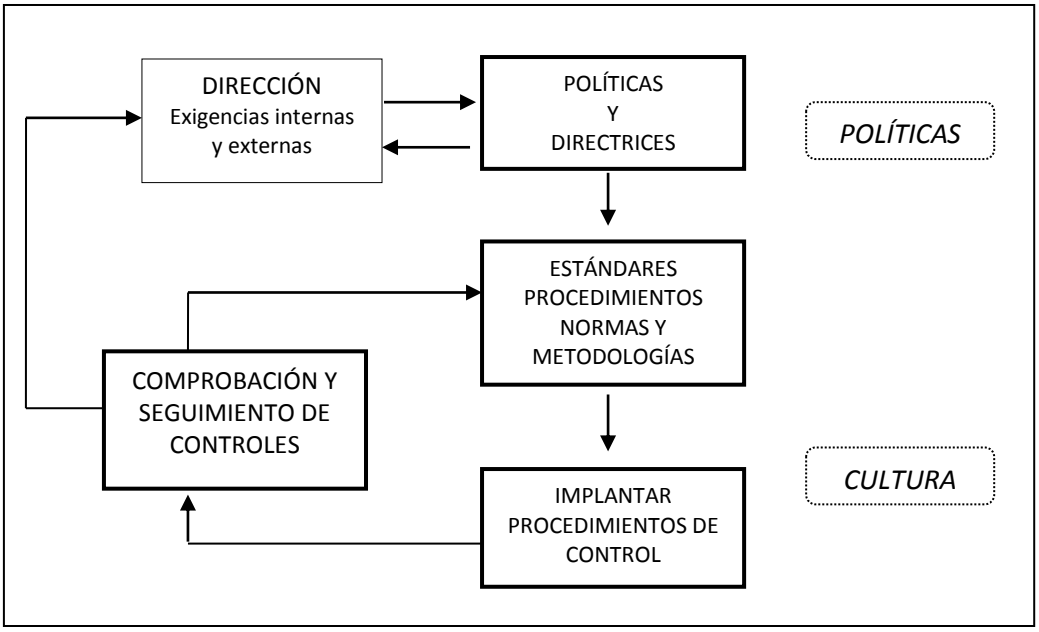


Figura II.5 Funcionamiento del Control Interno Informático

- **Auditor Externo/Interno Informático:** revisa los diferentes controles internos definidos en cada una de las funciones informáticas y el cumplimiento de normativa interna y externa, de acuerdo al nivel de riesgo, conforme a los objetivos definidos por la Dirección de Negocio y la Dirección de Informática. Informará a la Alta Dirección de los hechos observados y al detectarse deficiencias o ausencias de controles recomendarán acciones que minimicen los riesgos que pueden originarse.

La creación de un sistema de control informático es una responsabilidad de la Gerencia y un punto destacable de la política en el entorno informático.

A continuación se indican algunos controles internos para un Sistema de Información, agrupados por secciones funcionales y que serían los que Control Interno Informático y Auditoría Informática deberían verificar para determinar su cumplimiento y validez:

1. Controles generales organizativos:

- Políticas: deberán servir de base para la planificación, control y evaluación por la Dirección de las actividades del Área Informática.
- Planificación:
  - *Plan Estratégico de Información*, realizado por los órganos de la Alta Dirección de la Empresa donde se definen los procesos corporativos y se considera el uso de las diversas TI así como las amenazas y oportunidades de su uso o de su ausencia.
  - *Plan Informático*, realizado por el Departamento de Informática, determina los cambios precisos para cubrir las necesidades de la empresa plasmándolas en proyectos informáticos.
  - *Plan General de Seguridad (física y lógica)*, que garantice la confidencialidad, integridad y disponibilidad de la información.
  - *Plan de Emergencia Ante Desastres*, que garantice la disponibilidad de los sistemas ante eventos.
- Estándares: que regulen la adquisición de recursos, el diseño, desarrollo y modificación y explotación de sistemas.
- Procedimientos: que describan la forma y las responsabilidades de ejecutoría para regular las relaciones entre el Área Informática y los departamentos usuarios.
- Organizar el Área informática en un nivel suficientemente superior de estructura organizativa como para asegurar su independencia de los departamentos usuarios.
- Descripción de las funciones y responsabilidades dentro del Área Informática con clara separación de las mismas.
- Políticas de personal: selección, plan de formación, plan de vacaciones y evaluación y promoción.
- Asegurar que la Dirección revisa todos los informes de control y resuelve las excepciones que ocurran.
- Asegurar que existe una política de clasificación de la información para saber dentro de la Organización que personas están autorizadas y a qué información.

- Designar oficialmente la figura de Control Interno Informático y de Auditoría Informática (estas dos figuras se nombrarán internamente en base al tamaño del departamento de Informática).

2. Controles de desarrollo, adquisición y mantenimiento de Sistemas de Información:

Para que permitan alcanzar la eficacia del sistema, economía y eficiencia, integridad de los datos, protección de los recursos y cumplimiento con las leyes y regulaciones.

- Metodología del ciclo de vida del desarrollo de sistemas: su empleo podrá garantizar al Alta Dirección que se alcanzarán los objetivos definidos para el sistema. Estos son algunos controles que deben existir en la metodología:
  - La Alta Dirección debe publicar una normativa sobre el uso de metodología del ciclo de vida del desarrollo de sistemas y revisar ésta periódicamente.
  - La metodología debe establecer los papeles y responsabilidades de las distintas áreas del departamento de Informática y de los usuarios, así como la composición y responsabilidades del equipo del proyecto.
  - Las especificaciones del nuevo sistema deben ser definidas por los usuarios que dar escritas y aprobadas antes de que comience el proceso de desarrollo.
  - Debe establecerse un estudio tecnológico de la viabilidad en el cual se formulen formas alternativas de alcanzar los objetivos del proyecto acompañadas de un análisis costo-beneficio de cada alternativa.
  - Cuando se seleccione una alternativa debe realizarse el plan director del proyecto. En dicho plan deberá existir una metodología de control de costos.
  - Procedimientos para la definición y documentación de especificaciones de diseño, de entrada, de salida, de archivos, de procesos, de programas de controles de seguridad, de pistas de auditoría, etc.
  - Plan de validación, verificación y pruebas.
  - Estándares de prueba de programa, de prueba de sistemas.
  - Plan de conversión: prueba de aceptación final.
  - Los procedimientos de adquisición de software deberán seguir las políticas de adquisición de la Organización y dichos productos debieran ser probados y revisados antes de pagar por ellos y ponerlos en uso.
  - La contratación de programas de servicios de programación a medida ha de estar justificada mediante una petición escrita de un director de proyecto.

- Deberán prepararse manuales de operación y mantenimiento como parte de todo proyecto de desarrollo o modificación de sistemas de información, así como manuales de usuario.

- Explotación y mantenimiento: el establecimiento de controles asegurará que los datos se tratan de forma congruente y exacta y que el contenido de sistemas sólo será modificado mediante autorización adecuada. Estos son algunos de los controles que se deben implantar:
  - Procedimientos de control de explotación.
  - Sistema de contabilidad para asignar a usuarios los costos asociados con la explotación de un SI.
  - Procedimiento para realizar un seguimiento y control de los cambios de un SI.

3. Controles de explotación de Sistemas de Información:

- Planificación y gestión de recursos: definir el presupuesto operativo del Departamento, Plan de adquisición de equipos y gestión de la capacidad de los equipos.
- Controles para usar, de manera efectiva los recursos de computadores:
  - Calendario de carga de trabajo.
  - Programación de personal.
  - Mantenimiento preventivo del material.
  - Gestión de problemas y cambios.
  - Procedimientos de facturación a usuarios.
  - Sistemas de gestión de la biblioteca de soportes.
  - Procedimientos de selección del software del sistema, de instalación, de mantenimiento, de seguridad y control de cambios.
- Seguridad física y lógica:
  - Definir un grupo de seguridad de la información, siendo una de sus funciones la administración y gestión del software de seguridad, revisar periódicamente los informes de violaciones y actividad de seguridad para identificar y resolver incidentes.
  - Controles físicos para asegurar que el acceso a las instalaciones del Departamento de Informática queda restringido a las personas autorizadas.
  - Las personas externas a la Organización deberán ser acompañadas por un miembro de la plantilla cuando tengan que entrar en las instalaciones.

- Instalación de medidas de protección contra el fuego.
- Formación y concienciación en procedimientos de seguridad y evacuación del edificio.
- Control de acceso restringido a los computadores mediante la asignación de un identificador de usuario con palabra clave personal e intransferible.
- Normas que regulen el acceso a los recursos informáticos.
- Existencia de un plan de contingencias para el respaldo de recursos de computador críticos y para la recuperación de los servicios del Departamento Informático después de una interrupción imprevista de los mismos.

4. Controles en aplicaciones:

Cada aplicación debe llevar controles incorporados para garantizar la entrada, actualización, validez y mantenimiento completo y exacto de los datos. Las cuestiones más importantes en el control de los datos son:

- Control de entrada de datos: procedimientos de conversión y de entrada. Validación y corrección de datos.
- Controles de tratamientos de datos para asegurar que no se dan de alta, modifican o barran datos no autorizados para garantizar la integridad de los mismos mediante procesos no autorizados.
- Controles de salidas de datos: sobre el cuadre y reconciliación de salidas, procedimientos de distribución de salidas, de gestión de errores en las salidas, etc.

5. Controles específicos de tecnologías:

- Controles en Sistemas de Gestión de Base de Datos.
  - El software de gestión de base de datos para prever el acceso a, la estructuración de, y el control sobre los datos compartidos, deberá instalarse y mantenerse de modo tal que asegure la integridad del software, las bases de datos y las instrucciones de control que definen el entorno.
  - Que están definidas las responsabilidades sobre la planificación, organización, dotación y control de los activos de datos, es decir, un administrador de datos.
  - Que existen procedimientos para la descripción y los cambios de datos así como para el mantenimiento del diccionario de datos.
  - Controles sobre el acceso a datos y de concurrencia.
  - Controles para minimizar fallos, recuperar el entorno de las bases de datos hasta el punto de la caída y minimizar el tiempo necesario para la recuperación.

- Controles para asegurar la integridad de los datos: programas de utilidad para comprobar los enlaces físico-punteros- asociados a los datos, registros de control para mantener los balances transitorios de transacciones para su posterior cuadre con totales generados por el usuario o por otros sistemas.

- Controles en informática distribuida y redes:
  - Planes adecuados de implementación, conversión y pruebas de aceptación para la red.
  - Existencia de un grupo de control de red.
  - Controles para asegurar la compatibilidad de conjunto de datos entre aplicaciones cuando la red es distribuida.
  - Procedimientos que definan las medidas y controles de seguridad a ser usados en la red de informática en conexión con la distribución del contenido de bases de datos entre los departamentos que usan la red.
  - Que se identifican todos los conjuntos de datos, sensibles de la red y que se han determinado las especificaciones para su seguridad.
  - Existencia de inventario de todos los activos de la red.
  - Procedimientos de respaldo del hardware y del software de la red.
  - Existencia de mantenimiento preventivo de todos los activos.
  - Que existen controles que verifican que todos los mensajes de salida se validan de forma rutinaria para asegurar que contienen direcciones de destino válidas.
  - Controles de seguridad lógica: control de acceso a la red, establecimiento de perfiles de usuario.
  - Procedimientos automáticos para resolver cierres del sistema.
  - Monitorización para medir la eficiencia de la red.
  - Diseñar el trazado físico y las medidas de seguridad de las líneas de comunicación local dentro de la organización.
  - Detectar la correcta o mala recepción de mensajes.
  - Revisar los contratos de mantenimiento y el tiempo medio de servicios acordados con el proveedor con objeto de obtener una cifra de control constante.
  - Determinar si el equipo multiplexor/concentrador/procesador frontal remoto tiene lógica redundante y poder de respaldo con realimentación automática para el caso de que falle.
  - Asegurarse de que haya procedimientos de recuperación y reinicio.

  - Asegurarse de que existan pistad e auditoría que puedan usarse en la reconstrucción de los archivos de datos y de las transacciones de los diversas terminales. Debe existir la capacidad de rastrear los datos entre la terminal y el usuario.
  - Considerar circuitos de conmutación que usen rutas alternativas para diferentes paquetes de información provenientes del mismo mensaje; esto ofrece una forma de seguridad en caso de que alguien intercepte los mensajes.
- Controles sobre computadores personales y redes de área local.
  - Políticas de adquisición y utilización.
  - Normativas y procedimiento de desarrollo y adquisición de software de aplicaciones.
  - Procedimiento de control de software contratado bajo licencia.
  - Controles de acceso a redes, mediante palabra clave, a través de computadores personales.
  - Revisiones periódicas del uso de los computadores personales.
  - Políticas que contemplen la selección, adquisición e instalación de redes de área local.
  - Procedimientos de seguridad física y lógica.
  - Departamento que realice la gestión y soporte técnico de la red. Controles para evitar modificar la configuración de una red. Recoger información detallada sobre los Minis existentes: Arquitectura (CPU´s, Discos, Memoria, Streamer, Terminales, etc.), Conectividad (LAN, mini to host, etc), Software (sistema operativo, utilidades, lenguajes, aplicaciones, etc). Servicios soportados.
  - Inventarios actualizados de todas las aplicaciones de la Entidad.
  - Política referente a la organización y utilización de los discos duros de los equipos, así como para la nomenclatura de los archivos que contienen y verificar que contiene al menos: obligatoriedad de etiquetar el disco dura con el número de serie del equipo, creación de su subdirectorio por usuario en el que se almacenarán todos sus archivos privados, así como creación de un subdirectorio público que contendrá todas las aplicaciones de uso común para los distintos usuarios.
  - Implantar herramientas de gestión de la red con el fin de valorar su rendimiento, planificación y control.

- Procedimientos de control de los file-transfer que se realizan y de controles de acceso para los equipos con posibilidad de comunicación. Políticas que obliguen a la desconexión de los equipos de las líneas de comunicación cuando no se está haciendo uso de ellas.
- Adoptar los procedimientos de control y gestión adecuados para la integridad, privacidad, confidencialidad y seguridad de la información contenida en redes del área local.
- Cuando exista conexión PC-Host, comprobar que opera bajo los controles necesarios para evitar la carga/extracción de datos de forma no autorizada.
- Contratos de mantenimiento (tanto preventivo como correctivo o detectivos).
- Cuando en las acciones de mantenimiento se requiera la acción de terceros o la salida de los equipos de los límites de la oficina, se deberán establecer procedimientos para evitar la divulgación de información confidencial o sensible.
- Mantener un registro documental de las acciones de mantenimiento realizadas, incluyendo la descripción del problema y la solución dada al mismo.
- Los computadores deberán estar conectados a equipos de continuidad (UP´s, grupo, etc.)
- Protección contra incendios, inundaciones o electricidad estática.
- Control de acceso físico a los recursos microinformáticos: llaves de PC´s. Áreas restringidas. Ubicación de impresoras (propias y de red). Prevención de robos de dispositivos. Autorización para desplazamientos de equipos. Acceso físico fuera de horario normal.
- Control de acceso físico a los datos y aplicaciones: almacenamiento de disquetes con copias de backup u otra información o aplicación, procedimientos de destrucción de datos e informes confidenciales, identificación de disquetes/cintas, inventario completo de disquetes almacenados, almacenamiento de documentación.
- En los computadores en que se procesen aplicaciones o datos sensibles instalar protectores de oscilación de línea eléctrica y sistemas de alimentación ininterrumpida.
- Implantar en la red local productos de seguridad así como herramientas y utilidades de seguridad.
- Control de las conexiones remotas in/out (CAL): Modems, gateways, Mapper.

- Procedimientos para la instalación o modificación de software y establecer que la dirección es consciente del riesgo de virus informático y otros software maliciosos, así como de fraude por modificaciones no autorizadas de software y daños.
- Control para evitar la introducción de un sistema operativo que pudiera vulnerar el sistema de seguridad establecido.

II.1.5 Control Interno Informático-Auditoría Informática [9]

Es posible marcar las diferencias y similitudes de estos dos conceptos. En la Tabla II.2 Diferencia Control Interno Informático – Auditor Informático se presenta a manera de resumen estas dos cuestiones.

Tabla II.2 Diferencia Control Interno Informático – Auditor Informático

	CONTROL INTERNO INFORMÁTICO	AUDITOR INFORMÁTICO
SIMILITUDES	- Personal interno - Conocimientos especializados en Tecnología de la Información. - Verificación del cumplimiento de controles internos, normativas y procedimientos establecidos por la Dirección de Informática y la Dirección General para los sistemas de información.	
DIFERENCIAS	- Análisis de los controles en el día a día. - Informa a la Dirección del Departamento de Informática. - Solo personal interno. - El alcance de sus funciones es únicamente sobre el Área Informática.	- Análisis de un momento informático determinado. - Informa a la Dirección General de la Organización. - Personal interno y/o externo. - Tiene cobertura sobre todos los componentes de los sistemas de información de la organización.

II.1.6 Gobierno de Tecnología de Información (GTI)

Se entiende por GTI, el conjunto de acciones que realiza el área de TI en coordinación con la alta dirección para movilizar sus recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o del negocio. [1]

Constituye una parte esencial del gobierno de la empresa en su conjunto y aglutina la estructura organizativa y directiva necesaria para asegurar que TI soporta y facilita el desarrollo de los objetivos estratégicos definidos.

El IT Governance Institute señala que "El GTI es responsabilidad del Consejo de Administración y la alta dirección. Es una parte integral del gobierno corporativo y consiste en que el liderazgo, las estructuras organizativas y los procesos, aseguren que la TI sostiene y extiende los objetivos y estrategias de la Organización". Por tanto, el GTI tiene que ver, sobre todo con la capacidad de la toma de decisiones, la supervisión y el control de las TI. [1]

El GTI garantiza que:

- TI está alineada con la estrategia del negocio.
- Los servicios y funciones de TI se proporcionan con el máximo valor posible o de la forma más eficiente.
- Todos los riesgos relacionados con TI sean conocidos y administrados y los recursos de TI están seguros.

En la definición anterior, la clave es "*alinear*"; este término, expresado de forma sencilla, describe la dirección y fuerza global resultante al tomar como conjunto una serie de elementos dispares. En lo relativo al GTI, se refiere a buscar que cada una de las áreas de la Organización tire hacia una misma dirección y obtener una mejor fuerza global resultante. (Ver Figura II.6 Dirección de Objetivos – Fuerza Resultante)

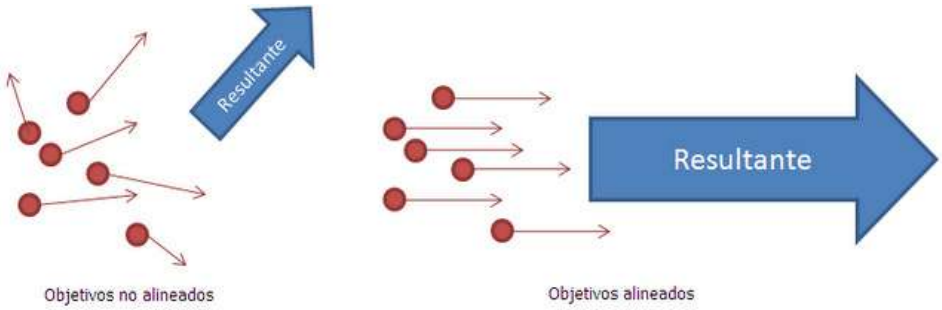


Figura II.6 Dirección de Objetivos – Fuerza Resultante

Cuando hablamos de GTI hacemos referencia a <11>:

- **Alineamiento Estratégico**: Las TI deben diseñarse desde el principio para apoyar y soportar la estrategia de la Organización, estableciendo prioridades que enlacen claramente los planes de TI con los objetivos estratégicos de la compañía, identificando responsabilidades y tareas.

- **Entrega de Valor**: Se trata de ejecutar el plan estratégico y **demostrando** que TI está efectivamente ofreciendo beneficios a la organización. También habla de la

optimización de compras, pero aquí desde el punto de vista estratégico, es decir, no se trata sólo de que el gasto sea óptimo, sino de validar si éste gasto es el necesario, de forma *razonada*.

- **Gestión de Recursos**: Su objetivo es la definición y gestión eficiente de los recursos de TI, lo que suele incluir aplicaciones, información, infraestructuras y por supuesto, personas. En este punto también se presta especial atención a algunos elementos clave, como la optimización del conocimiento y de las infraestructuras.

- **Gestión de Riesgos**: Las principales regulaciones obligan a la alta dirección a conocer el *riesgo operativo* al que se enfrenta la organización, y de aceptar el riesgo residual que se decidan.

- **Medición del rendimiento**: Trata de medir y conocer en todo momento el estado y grado de implementación de la estrategia o plan definido, de acuerdo a las cambiantes necesidades de la organización. Para ello se deben monitorizar de forma regular elementos como el estado de los proyectos, rendimiento de los procesos, uso de recursos y aspectos económicos o entrega del servicio.

II.1.7 Normas y Técnicas Internacionales

Un GTI, éste debe apoyarse en un marco de estándares y normas de comportamiento para garantizar que las Tecnologías de Información soporte los objetivos de negocio de la organización. A estas alturas del siglo XXI nadie duda que la implantación de metodologías como:

- Information Technology Infrastructure Library (ITIL), que da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI.
- Six Sigma, es una metodología de mejora de procesos, centrada en la reducción de la variabilidad de los mismos, consiguiendo reducir o eliminar los defectos o fallos en la entrega de un producto o servicio al cliente. Six Sigma utiliza herramientas estadísticas para la caracterización y el estudio de los procesos, de ahí el nombre

de la herramienta, ya que sigma es la desviación típica que da una idea de la variabilidad en un proceso y el objetivo de la metodología sigma es reducir ésta de modo que el proceso se encuentre siempre dentro de los límites establecidos por los requisitos del cliente.

Estas metodologías han contribuido a la mejora en la Gestión de TI. Año tras año vemos como cada vez hay más empresas certificadas en normas de Gestión de Servicios de TI como ISO-20000 o normas de Gestión de la Seguridad de la Información como ISO-27000. Ahora bien, ¿existen Normas y Metodologías para apoyar el GTI?

La primera norma internacional que trata sobre el concepto de GTI es ISO/IEC-38500. La norma busca asesorar a quienes tienen responsabilidades sobre el correcto funcionamiento de las organizaciones, en relación al papel que les toca jugar respecto de las TI , definiendo y detallando unos principios generales para el buen Gobierno Corporativo de las TI: responsabilidad, estrategia, inversión, conformidad, rendimiento y comportamiento.

Respecto a las metodologías, no existe una metodología unificada para el GTI. Existen metodologías que ayudan y facilitan un buen GTI, destacando principalmente ITIL y COBIT por los años que llevan incorporando las mejores prácticas en Gestión y GTI.

- ITIL es un marco de trabajo basado en mejores prácticas. En su nueva Versión 3 se centra en integrar las TI con el negocio, incorporando mejores prácticas para el GTI y adoptando un punto de vista más estratégico, reforzándolo con la ampliación de los procesos de Estrategia de Servicio. Se ha convertido en un estándar de facto.

- COBIT es un marco de trabajo aceptado internacionalmente como una buena práctica para el control de la información TI y los riesgos que conllevan. Permite a los gerentes cubrir la brecha entre los requerimientos de control, los aspectos técnicos y riesgos de negocio. Realza la importancia en cuanto a regulaciones, estando implantado en grandes empresas que cotizan en bolsa y prácticamente imprescindible para las que cotizan en Wall Street.

También hay marcos de trabajo que tratan más específicamente algunos aspectos relativos al GTI. Entre ellos cabe destacar:

- Val IT que se concentra en la gestión del portfolio de iniciativas de TI para generar valor a la organización y proveer un marco de trabajo para el gobierno de las inversiones en TI.

- RISK IT establece un marco de trabajo para las organizaciones para identificar, gobernar y administrar los riesgos asociados a las iniciativas en TI.

Con el propósito de integrar o relacionar todos los marcos e iniciativas de ISACA (Information Systems Audit and Control Association), que es una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información, así como conectar con el resto de iniciativas y estándares aceptados en la comunidad TI (ITIL, ISO, etc.), se está preparando COBIT 5. Aunque, a priori, es una buena noticia la integración de los diferentes marcos y metodologías, será difícil tener un único marco de trabajo que nos sirva para todo, dada la complejidad de los aspectos de la GTI. Deberemos esperar hasta principios del año que viene para poder evaluar todas las novedades que aporta al GTI el nuevo COBIT 5.

II.1.7.1 COBIT.

Desarrollado por la Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI), COBIT (Control Objectives for Information and related Technology) es el modelo para el GTI. [1]

Independientemente de la realidad tecnológica de cada caso concreto, COBIT determina, con el respaldo de las principales normas técnicas internacionales, un conjunto de mejores prácticas para la seguridad, la calidad, la eficacia y la eficiencia en TI que son necesarias para alinear TI con el negocio, identificar riesgos, entregar valor al negocio, gestionar recursos y medir el desempeño, el cumplimiento de metas y el nivel de madurez de los procesos de la organización.

COBIT es un estándar que permite evaluar la calidad del soporte de TI actual de la organización, vinculando los distintos procesos del negocio con los recursos informáticos que los sustentan, y los requerimientos sobre la información de los primeros. COBIT está diseñado para ser la herramienta de gobierno de TI que ayude al entendimiento y a la administración de los riesgos así como de los beneficios asociados con la información y sus tecnologías relacionadas.[1]

COBIT tiene como misión investigar, desarrollar, publicar y promover un conjunto de objetivos de control en TI con autoridad, actualizados, de carácter internacional y aceptado generalmente para el uso cotidiano de gerentes de empresas y auditores.

COBIT está diseñado para ser utilizado por tres tipos de destinatarios:

- ADMINISTRACION/ GERENCIA: Para ayudarlos a lograr un balance entre los riesgos y las inversiones en control en un ambiente de TI frecuentemente impredecible.
- USUARIOS: Para obtener una garantía en cuanto a la seguridad y controles de los servicios de tecnología de información proporcionados internamente o por terceras partes.
- AUDITORES: Para soportar su opinión y/o proporcionar consejos a la Administración sobre los controles internos.

II.1.7.1.1 Estructura de COBIT: [1]

El estándar COBIT posee tres niveles, llamados: Dominios, Procesos y Actividades.

En el nivel más elevado están los dominios, que son agrupamientos de procesos conforme a la naturaleza de estos. Los cuatro dominios principales son:

- **Planificación y Organización** – Este dominio agrupa los controles a nivel estratégico y táctico, e identifica la manera a través de la cual se puede lograr la mejor contribución de TI en el alcance de las metas y objetivos de negocio. Obviamente, la definición de la planificación estratégica de la organización debe contemplar requerimientos que surgen de diferentes puntos de vista, y su comunicación y gerenciamiento deben ser realizados según distintas perspectivas.
- **Adquisición e Implementación** – Para llevar adelante con éxito la estrategia del área de TI, las necesidades de soluciones tecnológicas deben ser identificadas, desarrolladas o adquiridas, e implementadas. Asimismo, los cambios y el mantenimiento de dichas soluciones son igualmente importantes que las actividades antes mencionadas y también forman parte de este dominio, a partir de la consideración de todos los objetivos de control vinculados a estos temas.
- **Servicios y Soporte** – A este dominio conciernen todas las actividades involucradas a la prestación de servicio de parte del área de TI, desde su puesta en producción hasta el soporte posterior. Por lo tanto se incluyen las tareas de operación del equipamiento tecnológico, seguridad de la información, planificación de la continuidad de las operaciones y capacitación del staff, entre otras. Este

domino deberá abarcar todas aquellas actividades requeridas a los efectos de poder brindar el soporte tecnológico que necesita la organización.

- **Monitoreo –** Todos los procesos de TI requieren ser evaluados regularmente en relación a los tiempos de ejecución, calidad y cumplimiento de los requerimientos de control. Este dominio concentra las actividades gerenciales de control y controles independientes de parte de auditoría interna y externa, y cualquier otra actividad de control de otro origen.

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

En el próximo nivel se encuentran los procesos. Estos están formados por un conjunto de actividades o tareas, donde cada conjunto (proceso) posee características propias asociadas al control. El estándar posee treinta y cuatro procesos de TI, y en cada uno de estos procesos posee un objetivo de control de alto nivel.

En el nivel más bajo de la estructura están las actividades o tareas necesarias para alcanzar un resultado medible. Por cada uno de los treinta y cuatro procesos de TI del marco referencial, hay desde tres hasta treinta objetivos de control detallados, para un total de trescientos dieciocho. Los objetivos de control detallado contiene sentencias de los resultados deseados o propósitos a ser alcanzados mediante la implementación de procedimientos de control específicos en una actividad de TI, de esta manera provee políticas claras y buenas prácticas para los controles de TI. Esta estructura cubre todos los aspectos de información y la Tecnología que la soporta.

En resumen, con el fin de proveer la información que la organización necesita para lograr sus objetivos, el GTI debe ser entrenado por la organización para asegurar que los recursos de TI serán administrados por una colección de procesos de TI agrupados naturalmente. La Figura II.7 Procesos de COBIT ilustra este concepto.

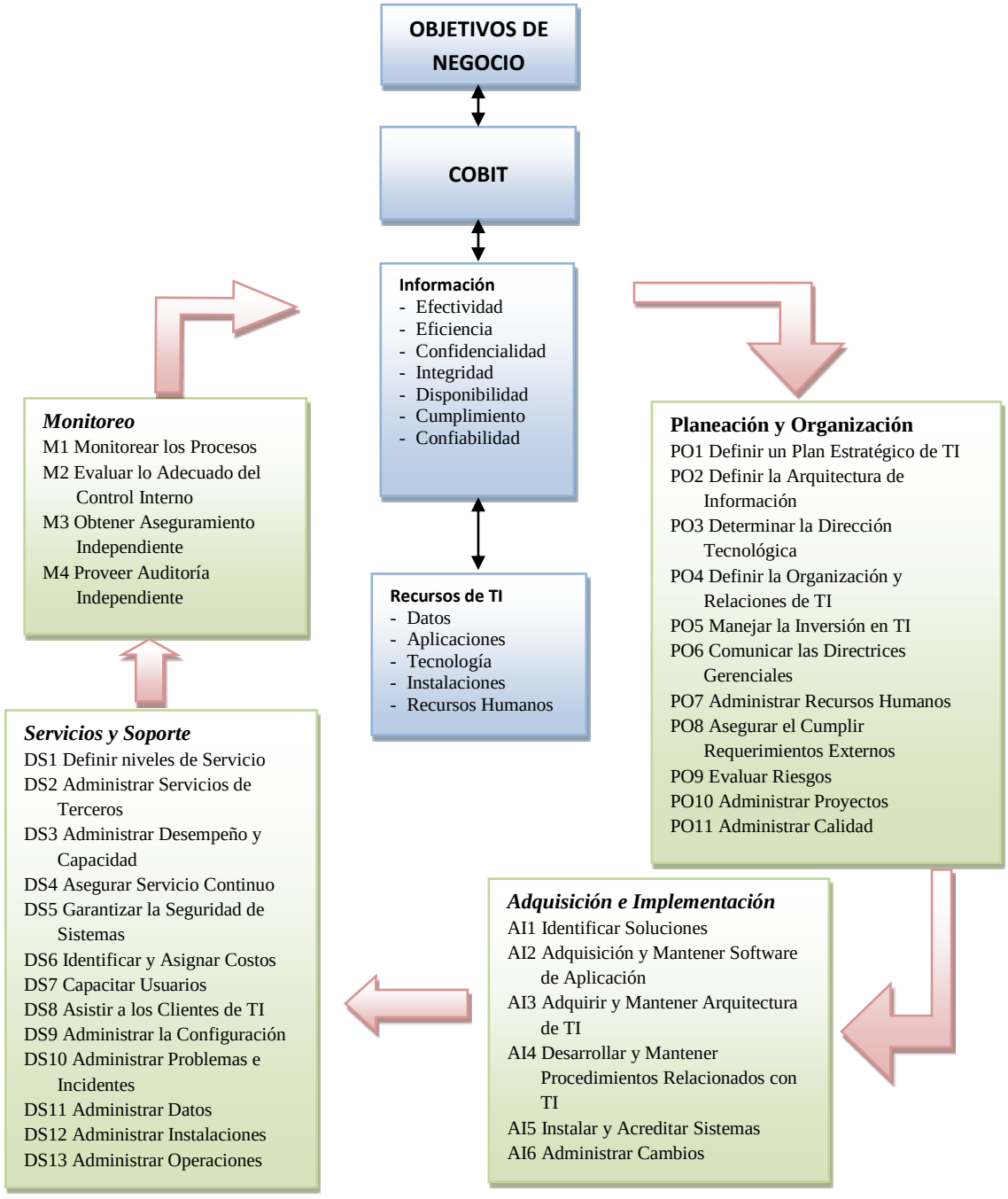


Figura II.7 Procesos de COBIT

II.1.7.1.2 Criterio de Información y Recursos de TI [1]

Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que COBIT hace referencia como requerimientos de negocio para la información. Al establecer la lista de requerimientos, COBIT combina los principios contenidos en los modelos referenciales existentes y conocidos:

- **Requerimiento de Calidad**: Calidad, Costo, Entrega de Servicio.
- **Requerimientos Fiduciarios:** Efectividad y Eficiencia de Operaciones, Confiabilidad de la Información, Cumplimiento de las Leyes y Regulaciones.
- **Requerimientos de Seguridad**: Confidencialidad, Integridad, Disponibilidad.

Cuando se hace mención al **requerimiento de Calidad**, se hace referencia a lo que el negocio siempre ha solicitado, calidad en la generación de información, es decir, con calidad se busca que la información no tenga fallas, que sea confiable, y que provea un desempeño más allá de las expectativas. Un aspecto importante de la calidad es que la información sea efectiva, es decir, que alcance el objetivo para el cual fue planteada.

El costo de la información también es importante, por lo que siempre se busca eficiencia en la información a través de una manejo adecuado de los recursos y lograr los objetivos con el mínimo uso de recursos posible.

Los **requerimientos Fiduciarios** se refieren a satisfacer los objetivos del negocio independientemente de las TI. Dentro del marco de referencia de COBIT, los requerimientos fiduciarios buscan satisfacer "efectividad y eficiencia de operaciones, confiabilidad de la información, y cumplimiento de las leyes y regulaciones".

Entonces se buscan eficiencia y eficacia de la información, además se requiere una confiabilidad de la información para la administración financiera del negocio. Sin embargo los requerimientos fiduciarios agregan algo nuevo, que se refiere a cumplir los reglamentos, leyes y obligaciones para una correcta provisión de información.

Para el **requerimiento de Seguridad,** la organización busca mantener su información segura y protegida de cualquier eventualidad, ataque, o acceso no autorizado que pueda poner en peligro el funcionamiento del negocio y el contenido de los datos.

COBIT identifica confidencialidad como un elemento importante para garantizar que la información sea restringida. También se requiere que la información sea válida y que refleje la realidad del negocio, es decir, integridad de la información. Para terminar se menciona nuevamente la disponibilidad como un elemento clave para poder acceder a la información cuando se la necesita.

Estas tres categorías muestran distintas necesidad, inclusive donde se puede apreciar como algunas se superponen y otras son independientes, pero la importancia radica en que son necesidades que tiene el negocio y que espera estas características de la información.

Luego del análisis de requerimientos en varias empresas e industrias del mundo, se identificaron siete requerimientos claves de negocio acerca de la información, los cuales fueron denominados como criterios de información. Un criterio de información se define como "un requerimiento de negocio para la información". En otras palabras son las características que el negocio espera que toda información tenga para estar seguro de tomar buenas decisiones. A continuación se listan los siete criterios de información definidos por dentro de los principios del Marco de Referencia de COBIT:

- **Efectividad:** Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
- **Eficiencia:** Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
- **Confidencialidad:** Se refiere a la protección de información sensible contra divulgación no autorizada.
- **Integridad:** Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
- **Disponibilidad:** Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
- **Cumplimiento:** Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.
- **Confiabilidad de la Información:** Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Los **recursos de TI** identificados en COBIT pueden explicarse/definirse como se muestra a continuación:

- **Datos:** Son objetos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.

- **Sistemas de Aplicación:** Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.
- **Tecnología:** La tecnología cubre hardware, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.
- **Instalaciones:** Recursos para alojar y dar soporte a los sistemas de información.
- **Personal:** Habilidades del personal, conocimiento, sensibilización y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

II.1.7.1.3 Relación Procesos de TI - Criterios de Información

En la Tabla II.3 Relación Procesos de TI - Criterios de Información brinda una visión global de cómo se relacionan los procesos de TI con los criterios de información. La relación se evalúa teniendo en cuenta cómo impacta el criterio de información en el proceso de TI, basada en rigurosos informes y observaciones de procesos por parte de investigadores, expertos y revisores. Esta valoración puede ser:

- **Primario:** es el grado al cual el objetivo de control definido impacta directamente el requerimiento de información de interés.
- **Secundario:** es el grado al cual el objetivo de control definido satisface únicamente de forma indirecta o en menor medida el requerimiento de información de interés.
- **Blanco (vacío):** podría aplicarse; sin embargo, los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y/o por otro proceso.

II.1.7.1.4 Componentes de COBIT

La versión COBIT 4.0, opta por un empaquetamiento distinto a sus versiones anteriores, integrando en un único ejemplar llamado Marco de trabajo los siguientes componentes: Resumen Ejecutivo, Marco de Referencia, Objetivos de Control y Directrices Gerenciales. El Marco de Trabajo es el único componente de esta versión que está al alcance de cualquier usuario, los demás componentes se comercializan. A continuación se describen estos componentes [1]:

• **El Resumen Ejecutivo:** es un resumen informativo a los niveles superiores, sobre el GTI, está diseñado para ayudar a los ejecutivos a entender porque el GTI es importante, cuáles son sus intereses y sus responsabilidades para su administración.

Tabla II.3 Relación Procesos de TI - Criterios de Información

		Criterios de información						
Dominio	**Proceso**	**Efectividad**	**Eficiencia**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Cumplimiento**	**Confiabilidad**
Planeación y Organización								
PO1	Definir un Plan Estratégico de TI	P	S					
PO2	Definir la Arquitectura de Información	P	S	**S**	**S**			
PO3	Determinar la Dirección Tecnológica	P	S					
PO4	Definir la Organización y Relaciones de TI	P	S					
PO5	Manejar la Inversión en TI	P	P					S
PO6	Comunicar las Directrices Gerenciales	P					S	
PO7	Administrar Recursos Humanos	P	P					
PO8	Asegurar el Cumplir Requerimientos Externos	P					P	S
PO9	Evaluar Riesgos	S	S	**P**	**P**	**P**	S	S
PO10	Administrar Proyectos	P	P					
PO11	Administrar Calidad	P	P		**P**			S
Adquisición e Implementación								
AI1	Identificar Soluciones	P	S					
AI2	Adquisición y Mantener Software de Aplicación	P	P		**S**		S	S
AI3	Adquirir y Mantener Arquitectura de TI	P	P		**S**			
AI4	Desarrollar y Mantener Procedimientos relacionados con TI	P	P		**S**		S	S
AI5	Instalar y Acreditar Sistemas	P			**S**	**S**		
AI6	Administrar Cambios	P	P		**P**	**P**		S
Servicios y Soporte								
DS1	Definir niveles de servicio	P	P	**S**	**S**	**S**	S	S
DS2	Administrar Servicios de Terceros	P	P	**S**	**S**	**S**	S	S
DS3	Administrar Desempeño y Capacidad	P	P			**S**		
DS4	Asegurar Servicio Continuo	P	S			**P**		
DS5	Garantizar la Seguridad de Sistemas			**P**	**P**	**S**	S	S
DS6	Identificar y Asignar Costos		P					P
DS7	Capacitar Usuarios	P	S					
DS8	Asistir a los Clientes de TI	P						
DS9	Administrar la Configuración	P				**S**		S
DS10	Administrar Problemas e Incidentes	P	P			**S**		
DS11	Administrar Datos				**P**			P
DS12	Administrar Instalaciones				**P**	**P**		
DS13	Administrar Operaciones	P	P		**S**	**S**		
Monitoreo								
M1	Monitorear los procesos	P	S	**S**	**S**	**S**	S	S
M2	Evaluar lo adecuado del control Interno	P	P	**S**	**S**	**S**	S	S
M3	Obtener aseguramiento independiente	P	P	**S**	**S**	**S**	S	S
M4	Proveer auditoría independiente	P	P	**S**	**S**	**S**	S	S

• **Directrices Gerenciales**: son herramientas para ayudar a asignar responsabilidades, medir el desempeño, llevar a cabo benchmarks y manejar brechas en la capacidad. Las directrices ayudan a brindar respuestas a preguntas comunes de la administración: ¿Qué tan lejos podemos llegar para controlar la TI?, y ¿El costo justifica el beneficio? ¿Cuáles son los indicadores de un buen desempeño? ¿Cuáles son las prácticas administrativas clave a aplicar? ¿Qué hacen otros? ¿Cómo medimos y comparamos?

• **Marco de Referencia**: explica cómo COBIT organiza los objetivos de gobierno y las mejores prácticas de TI con base en dominios y procesos de TI, y los vincula a los requerimientos del negocio.

• **Objetivos de Control:** brinda objetivos a la dirección basados en las mejores prácticas genéricas para todas las actividades de TI.

Como la actualización de las Directrices de Auditoría no se ha publicado, para este trabajo se consulta las directrices de Auditoria de la versión anterior del estándar COBIT. [1]

II.1.7.1.5 Directrices de Auditoría [3]

Las Directrices de Auditoría ofrecen una herramienta complementaria para la fácil aplicación del Marco Referencial y los Objetivos de Control COBIT dentro de las actividades de Auditoría y Evaluación. El propósito de las Directrices de Auditoría es contar con una estructura sencilla para auditar y evaluar controles, con base en prácticas de Auditoría generalmente aceptadas y compatibles con el estándar COBIT.

Los objetivos y prácticas individuales varían considerablemente de organización a organización y existen muchos tipos de prácticas dedicados a actividades relacionadas con la Auditoría; por ejemplo auditores externos, auditores internos, evaluadores, revisores de calidad, y asesores técnicos.

Por estas razones, las Directrices de Auditoría tienen una estructura genérica y de alto nivel. Los auditores deben cumplir con algunos requerimientos generales para proporcionar a los directivos y a los poseedores de los procesos de negocios, seguridad y asesoría respecto a los controles en una organización: ofrecer una seguridad razonable de que se está cumpliendo con los objetivos de control correspondientes; identificar dónde se encuentran las debilidades significativas en dichos controles; justificar los riesgos que pueden estar asociados con tales debilidades, y finalmente, aconsejar a estos ejecutivos sobre las medidas correctivas que deben adoptarse. COBIT ofrece políticas claras y prácticas eficaces en materia de seguridad y control de información, así como tecnología asociada. Por tanto, las Directrices de Auditoría firmemente basados en los Objetivos de Control, toman la opinión del auditor a partir de la conclusión de Auditoría, remplazándola con criterios normativos. Estas Directrices de Auditoría proporcionan orientaciones para preparar planes de Auditoría que se integran al Marco COBIT y a los Objetivos de Control detallados. Deben ser usados conjuntamente con estos dos últimos, y a partir de ahí pueden desarrollarse programas específicos de Auditoría. Sin embargo, las Directrices no son exhaustivas ni definitivas. No pueden incluir todo ni ser aplicables a todo, así que deberán ajustarse a condiciones específicas.

Un objetivo de control de TI es una declaración del resultado o fin que se desea lograr al implantar procedimientos de control en una actividad de TI en particular. Los objetivos de control de COBIT son los requerimientos mínimos para un control efectivo de cada proceso de IT. Los objetivos de control detallados son sentencias genéricas de acciones de las mejores prácticas de administración mínimas para garantizar que el proceso se mantiene bajo control.

Las Directrices de Auditoría COBIT permiten al auditor cotejar los procesos específicos de TI con los Objetivos de Control COBIT recomendados para auxiliar a los directivos a identificar en qué casos los controles son suficientes, o para asesorarlos respecto a los procesos que requieren ser mejorados.

Desde el punto de vista de los directivos, los propietarios de los procesos harán las preguntas: ¿Estoy haciendo lo correcto?, y si no es así: ¿Qué puedo hacer para corregirlo? El Marco y las Directrices de Auditoría COBIT ayudarán a responder a estas preguntas.

II.1.8 Modelo de Madurez de Capacidades (CMM)

El SEI (Software Engineering Institute), es el instituto que creó y mantiene el modelo de calidad. El CMM (Capability Maturit y Model), este es un modelo de evaluación de los procesos de una organización. Fue desarrollado inicialmente para los procesos relativos al software. Establece una medida del progresos conforme avanza, en niveles de madurez. Cada nivel a su vez cuenta con un número de áreas claves de proceso (KPA-Key Process Area), que deben lograrse. El alcanzar estas áreas o estadios se detecta mediante la satisfacción o insatisfacción de varias metas claras y cuantificables. [13]

A su vez para cada área de proceso se define un conjunto de buenas prácticas que habrán de ser:

- Definidas en un procedimiento documentado.
- Provistas (la organización) de los medios y formación necesarios.
- Ejecutadas de un modo sistemático, universal y uniforme (institucionalizadas).
- Medibles o cuantificables.
- Verificadas.

Estas áreas de proceso se agrupan en distintos "niveles de madurez", de modo que una organización que tenga institucionalizadas todas las prácticas incluidas en un nivel y sus inferiores, se considera que ha alcanzado ese nivel de madurez.

Los niveles son:

1. **Inicial**. Las organizaciones en este nivel no disponen de un ambiente estable para el desarrollo y mantenimiento de software. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostos. El resultado de los proyectos es imprescindible. En los proyectos en este nivel los presupuestos se disparan, no es posible entregar en las fechas establecidas. No hay control sobre el estado del proyecto, el desarrollo del proyecto es completamente opaco.

   Si no se sabe el tamaño del proyecto y no se sabe cuánto se lleva hecho, nunca se sabrá cuando va a estar concluido.

2. **Repetible**. En este nivel las organizaciones disponen de prácticas institucionalizadas de gestión de proyectos, existen métricas básicas y un razonable seguimiento de la calidad. La relación con subcontratistas y clientes está gestionada sistemáticamente. Esto significa que el éxito de los resultados obtenidos se puede repetir. La principal diferencia entre este nivel y el anterior es que el proyecto es gestionado y controlado durante el desarrollo del mismo. El desarrollo no es opaco y se puede saber el estado del proyecto en todo momento.

   Los procesos que hay que implantar para alcanzar este nivel son:

   - Gestión de requisitos
   - Planificación de proyecto
   - Seguimiento y control de proyectos
   - Gestión de proveedores
   - Aseguramiento de la calidad
   - Gestión de la configuración

3. **Definido**. Además de una buena gestión de proyectos a este nivel las organizaciones disponen de correctos procedimientos de coordinación entre grupos,

formación del personal, técnicas de ingeniería más detallada y un nivel más avanzado de métricas en los procesos. Se implementan técnicas de revisión por pares.

Este nivel significa que la forma de desarrollar proyectos (gestión e ingeniería) está definida; por definida quiere decir que está establecida, documentada y que existen métricas (obtención de datos objetivos) para la consecución de objetivos concretos.

La mayoría de las empresas que llegan al nivel tres paran aquí, ya que es un nivel que proporciona muchos beneficios y no ven la necesidad de ir más allá porque tienen cubiertas sus necesidades.

4. **Gestionado**: Se caracteriza porque las organizaciones disponen de un conjunto de métricas significativas de calidad y productividad, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El software resultante es de alta calidad. Los proyectos usan objetivos medibles para alcanzar las necesidades de los clientes y la organización. Los procesos que hay que implantar para alcanzar este nivel son:
    - Gestión cuantitativa de proyectos
    - Mejora de los procesos de la organización
5. **Optimizado**: La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación. Los procesos de los proyectos y de la organización están orientados a las mejoras de las actividades. Mejoras incrementales e innovadoras de los procesos que mediante métricas son identificadas, evaluadas y puestas en práctica.

    Los procesos que hay que implantar para alcanzar este nivel son:

    - Innovación organizacional
    - Análisis y resolución de las causas

Normalmente las empresas que intentan alcanzar los niveles cuatro y cinco lo realizan simultáneamente ya que están muy relacionados.

Con la excepción del primer nivel, cada uno de los estantes Niveles de Madurez está compuesto por un cierto número de Áreas Claves de Proceso. [16][17]

II.1.8.1 Modelo de Madurez de Capacidades Integrado (CMMI)

El modelo CMM y el modelo CMMI (Capabilit y Maturity Model Integration) se diferencian básicamente en que el primero se enfoca principalmente a las organizaciones o áreas de Tecnologías de Información en cambio el modelo CMMI como su nombre lo indica es un modelo integrado y mejorado que se puede aplicar a un número mayor de organizaciones de diferentes sectores.

A partir del segundo nivel del modelo CMM se debe contar con áreas específicas que permitirán tener un mayor control del proyecto de software.

Para el nivel dos al menos se deberán contar con las siguientes áreas clave de proceso:

- Gestión de Requisitos
- Planificación del Proyecto de Software
- Seguimiento y Supervisión del Proyecto
- Gestión de subcontratos de Software
- Garantía de Calidad de Software
- Gestión de la configuración del software

Cada nivel va agregando nuevas Áreas Claves de Proceso.

De manera similar el CMMI también establece niveles para medir la capacidad de los procesos aunque para este modelo son seis:

0 No existe. El proceso no se realiza o no se consiguen los objetivos.

1 Inicial. El proceso se ejecuta y se logra el objetivo.

2 Repetible. Además de ejecutarse, el proceso se planifica, se revisa y se evalúa para comprobar que cumple los requisitos.

3 Definido. Además de ser un proceso gestionado se ajusta a la política de procesos que existe en la organización, alineada con directivas de la empresa.

4 Administrado. Además de ser un proceso definido se controla utilizando técnicas cuantitativas.

5 Optimizado. Además de ser un proceso cuantitativamente gestionado, de forma sistemática se revisa y modifica o cambia para adaptarlo a los objetivos de la organización. Mejora continua [18].

II.1.8.2 Beneficios del Modelo CMMI [19]

Los siguientes son los beneficios que el modelo CMMI proporciona a la organización:

- Administración de la información en forma clara y oportuna para atender necesidades operativas y de gestión.
- Efectividad en la detección temprana de errores a lo largo del ciclo de vida del desarrollo.
- Mayor tolerancia al cambio y adaptación de nuevas tecnologías.
- Comunicación efectiva entre todos los involucrados.
- Implementación de técnicas proactivas de gestión.
- Mejoramiento de selección y administración de proveedores.
- No es una estructura rígida, provee un esquema de trabajo consistente que permite nuevas iniciativas.
- Se enfoca con el problema del sistema total.
- Facilita la mejora en los procesos de toda la organización.
- Permite contar con un proceso sistematizado.
- Mejora la productividad en el desarrollo y gestión de proyectos, con un mayor ajuste a los plazos y costos esperados.

II.1.8.3 Diferencias Con el Modelo CMM

CMMI, es una evolución del modelo CMM el cual busca evaluar la madurez y con la Ingeniería de Sistemas, el Desarrollo Integrado de Productos, Procesos y la Administración de Proveedores de Servicios de Apoyo.

Este modelo no es aplicado en las grandes organizaciones, como en principio se podía creer, la tendencia está en buscar que un gran número de empresas pequeñas lo puedan implantar, aunque el gran obstáculo para la implementación de este modelo es el costo.

Entre CMM y CMMI otra de las diferencias que existe es que en CMM existen cinco niveles para clasificar a las organizaciones respecto a la madurez de sus procesos, cada uno de los cuales es una plataforma y requisito para avanzar al siguiente; mientras que en el modelo CMMI, tiene dos formas de representación; por estados, en el cual hay niveles consecutivos y representación continua, que permite que aquellas empresas mejoren sólo en alguna área de sus procesos.

Los procesos de evaluación de ambos son muy similares, aunque CMMI tiene un mayor grado de exigencia, al igual que el trabajo de recolección de evidencias y preparación de documentación. [20].

II.1.8.4 Evaluación del Nivel de Madurez de la Organización <14>

Muchas organizaciones valoran el medir su progreso llevando a cabo una evaluación y ganando una clasificación del nivel de madurez o de un nivel de capacidad de logro. Este tipo de evaluaciones son realizadas normalmente por una o más de las siguientes razones:

- Para determinar que tan bien los procesos de la organización se comparan con las mejores prácticas CMMI y determinar qué mejoras se pueden hacer.

Las valoraciones de las organizaciones utilizando un modelo CMMI deben ajustarse a los requisitos definidos en el documento "Appraisal Requirements for CMMI" (ARC). La evaluación se enfoca en identificar oportunidades de mejora, y comparar los procesos de la organización con las mejores prácticas CMMI. Los equipos de evaluación usan el modelo CMMI y un método conforme a ARC para guiar su evaluación y reporte de conclusiones. Los resultados de la evaluación son usados para planear mejoras en la organización.

El Standard CMMI Appraisal Method for Process Improvement (SCAMPI) es el método oficial SEI para proveer puntos de referencia de sistemas de calificación en relación con los modelos CMMI. SCAMPI se usa para identificar fortalezas y debilidades de los procesos, revelar riesgos de desarrollo/adquisición, y determinar niveles de capacidad y madurez. Se utilizan ya sea como parte de un proceso o programa de mejoramiento, o para la calificación de posibles proveedores. El método define el proceso de evaluación constando de preparación; las actividades sobre el terreno; observaciones preliminares, conclusiones y valoraciones; presentación de informes y actividades de seguimiento.

II.1.8.5 Conceptos Estadísticos

La estadística se puede definir como la ciencia que recopila, organiza, analiza e interpreta la información numérica o cualitativa, mejor conocida como datos, de manera que pueda llevar a conclusiones válidas.

- **Datos**: Son los valores cualitativos o cuantitativos mediante los cuales se miden las características de los objetos, sucesos o fenómenos a estudiar.

- **Entrevista y Encuesta**: Son métodos de recolección de datos, la entrevista es una serie de preguntas realizadas personalmente y la encuesta es llevada a cabo generalmente a través de algún formulario que la persona debe llenar.
- **Frecuencia**: Número de veces en que se repite un dato. Representado generalmente por fi.
- **Inferir**: Es emitir juicios o conclusiones basados en algún conocimiento o experiencia sobre un evento o suceso.
- **Moda**: Es el valor que más se repite en la muestra, es decir, es la observación que ocurre con mayor frecuencia en la muestra.

La moda muestra hacia qué valor tienden los datos a agruparse. En conjuntos relativamente pequeños, puede que no exista un par de observaciones cuyo valor sea el mismo. En esta situación no es clara la definición de moda.

También puede suceder que la frecuencia más alta se encuentre compartida por dos o más observaciones. En estos casos, la moda tiene una utilidad limitada como medida de tendencia central.

II.2. MARCO METODOLÓGICO

II. 2.1 Metodologías de Auditoria Informática

La AI debe respaldarse en un proceso formal que asegure su previo entendimiento por cada uno de los responsables de llevar a la práctica dicho proceso en la empresa. Al igual que otras funciones en el negocio, la AI efectúa sus tareas y actividades mediante una metodología.

II. 2.1.1 Clasificación de Metodologías de Auditoria Informática <11>

Existen algunas metodologías de AI y todas depende del alcance delo que se pretenda revisar o analizar y que proceso informático se va a auditar, además las metodologías para AI, en su gran mayoría, tienen procedimientos y tareas parecidos.

Para dar una clasificación de las metodologías de AI diremos que son de dos tipos:

- **Metodologías Generales**: Las metodologías generales permiten dar una opinión sobre la fiabilidad de la información, el resultado de esta metodología es un informe generalizado donde se destacan las vulnerabilidades encontradas. Es

importante conocer que este tipo de auditoría tiene como material de trabajo los checklist, (cuestionarios), entre otras que permiten anotar observaciones que ayudan a conservar un banco importante de pruebas sobre hallazgos.

- **Metodologías Específicas**: Las metodologías especificas son aquellas que el auditor interno o externo "crea" para su uso y son más específicas y exhaustivas, ya que sirve para evaluar un área en particular, al igual que la anterior metodología sus informes permiten el registro de observaciones.

Las metodologías para AI son parecidas pero no iguales, ya que poseen en general casi las mismas fases para un proceso de AI.

Para el desarrollo del presente trabajo de tesis se ha decidido analizar la metodología que se describe a continuación propuesta por Enrique Hernández, para realizar las modificaciones necesarias con el fin de adaptarla al Área de TI de la empresa de seguro.

II.2.1.2 Etapas de la Metodología de AI [11]

Hernández recomienda que la AI deba respaldarse por un proceso formal que asegure su previo entendimiento por cada uno de los responsables de llevar a la práctica dicho proceso en la empresa. Además sugiere que no es recomendable fomentar la dependencia, en el desempeño de esta función, en la experiencia, habilidades, criterios y conocimientos del auditor sino que debe existir una referencia metodológica. La función de la AI debe contar con un desarrollo de actividades basado en un método de trabajo formal, que sea entendido por las personas que van a ser auditoría y debe ser complementado con técnicas y herramientas propias de la función.

Es importante señalar que el uso de cualquier metodología de AI no garantiza por sí sola el éxito de los diferentes planes de AI se requiere también de un buen dominio y uso constante de los siguientes aspectos complementarios:

- Técnicas.
- Herramientas de productividad.
- Habilidades personales.
- Conocimientos técnicos y administrativos.
- Experiencia en los campos de AI.
- Conocimiento de los factores del negocio y del medio externo al mismo.
- Actualización permanente.

- Involucramiento y comunicación constante con asociaciones nacionales e internacionales relacionadas con el campo.

Esta Metodología propone seis etapas que son:

- Preliminar o Diagnóstico de la Situación Actual.
- Justificación.
- Adecuación.
- Formalización
- Desarrollo.
- Implantación.

Las cuales se describen a continuación:

Etapa Preliminar o Diagnostico de la situación actual: Esta etapa pretende conocer las opiniones de la alta dirección para estimar el grado de satisfacción y confianza que tiene en los productos, servicios y recursos de informática; así mismo, detecta las fortalezas, aciertos y apoyo que brinda dicha función desde la perspectiva de los directivos del negocio. El estudio preliminar de la situación actual también involucra al aspecto informático para lo cual se coordina directamente con el responsable de la función informática y se toma en consideración los siguientes temas:

- Estructura interna de informática.
- Funciones.
- Objetivos.
- Estrategias.
- Planes.
- Políticas.
- Tecnología de hardware y software en la que se apoya para llevar a cabo su función.
- Servicios que la función brinda a la organización.

Etapa de Justificación: En esta etapa se legitima la revisión o evaluación de las áreas o funciones críticas relacionadas con informática.

Los productos de esta etapa son:

- Matriz de riesgos.
- Plan general de auditoría informática.
- Compromiso ejecutivo.

Etapa de Adecuación: Esta etapa tiene como objetivo principal adaptar el proyecto a las características del negocio, sin olvidar la referencia de los estándares, políticas y procedimientos de auditoría comúnmente aceptados y recomendados por las asociaciones relacionadas con el proceso, así como las formuladas y aprobadas de manera particular en los negocios para informática. Al terminar la presente etapa, el auditor informático contará con un proyecto bien especificado y clasificado; en las etapas restantes solo se desarrolla e implanta lo definido.

En estas tres primeras etapas el autor pretende introducir al auditor informático en el negocio y sus diversas funciones para detectar las debilidades y fortalezas más relevantes; además se define la planeación y proyección de las áreas que requieren ser auditadas y se documenta las adecuaciones o agregados requeridos.

Etapa de Formalización: El proyecto adaptado a las características de la empresa será evaluado por la alta gerencia de la organización, la cual realiza las modificaciones en caso de ser necesario para brindar su apoyo a la realización de la AI.

Etapa de Desarrollo: En esta etapa se pone en práctica las actividades que se han proyectado. Esta etapa comprende:

- Concertación de fechas de entrevistas, visitas y aplicación de cuestionarios.
- Verificación de tareas, involucrados y productos terminados.
- Clasificación de técnicas, herramientas, cuestionarios y entrevistas.
- Aplicación de entrevistas y cuestionarios.
- Visitas de verificación.
- Elaboración del informe preliminar correspondiente a los componentes por áreas auditada.
- Revisión del informe preliminar.
- Clasificación y documentación del informe preliminar.
- Finalización de tareas o productos pendientes.
- Elaboración del informe final de la AI.
- Presentación a la alta dirección y participantes clave.
- Aprobación del proyecto y compromiso ejecutivo.

Etapa de Implantación: En esta etapa el trabajo de auditoría ha concluido ya que el auditor entregó el informe, consecuentemente, el personal que está involucrado con las

áreas afectadas toma conocimiento de las conclusiones y recomendaciones que se encuentran en el informe del auditor.

II.2.2 Metodologías de Gobierno de TI

Luego de realizar la lectura y el análisis de varios estudios sobre modelos de GTI, se llega a la conclusión que no existe una metodología unificada e integrada para GTI, tampoco un entendimiento común de que se trata.

Los estándar que ayudan y facilitan un buen GTI, son principalmente ITIL y COBIT, por los años que llevan incorporando las mejores prácticas en Gestión y Gobierno de TI.

- ITIL: es un marco de trabajo basado en mejores prácticas. En su nueva Versión 3 se centra en integrar las TI con el negocio, incorporando mejores prácticas para el Gobierno TI y adoptando un punto de vista más estratégico, reforzándolo con la ampliación de los procesos de Estrategia de Servicio.
- COBIT: es un marco de trabajo aceptado internacionalmente como una buena práctica para el control de la información TI y los riesgos que conllevan. Permite a los gerentes cubrir la brecha entre los requerimientos de control, los aspectos técnicos y riesgos de negocio.

También hay marcos de trabajo que tratan más específicamente algunos aspectos relativos al Gobierno de las TI. Entre ellos cabe destacar:

- Val IT que se concentra en la gestión del portfolio de iniciativas de TI para generar valor a la organización y proveer un marco de trabajo para el gobierno de las inversiones en TI.
- RISK IT establece un marco de trabajo para las organizaciones para identificar, gobernar y administrar los riesgos asociados a las iniciativas en TI. <13>

Como conclusión, se puede mencionar que no hay una metodología específica para el GTI, si no, Marcos de trabajo que indican que hacer, pero no como. De acuerdo con los expertos, sencillamente hemos de decir que son buenas prácticas que deben ajustarse a las necesidades de cada organización, aplicándolas basándose en la experiencia y el sentido común.

En este trabajo de investigación se desarrolla una propuesta metodológica del GTI para pequeñas y medianas empresas del medio que no disponen de una herramienta que permita

organizar las actividades necesarias para poder encausar la gobernabilidad de sus recursos de TI, luego es aplicada a la empresa bajo estudio adaptando la metodología a sus características y necesidades.

II.3 MARCO EMPIRICO

II.3.1 Descripción del Marco Empírico

El Marco Empírico facilita, en última instancia, la posibilidad de trazar una línea de evidencia entre las cuestiones propuestas inicialmente y las conclusiones finales del estudio.

El caso práctico será una empresa del medio que servirá de puente entre la formulación teórica de la metodología y la realidad; además, permitirá vislumbrar las posibilidades que ofrece la misma en posteriores aplicaciones.

II.3.2 Descripción de la Empresa

La organización es una empresa de servicios de seguro que tiene como actividad primordial brindar el servicio de asesoramiento de las personas y las empresas para la protección de la vida y su patrimonio.

Los objetivos que persigue son:

- Proporcionar un excelente servicio de protección a las personas y su patrimonio.
- Sostener un liderazgo en calidad, para asegurar en cada servicio que ofrece la satisfacción de sus clientes.
- Mantener o disminuir los costos y maximizar los beneficios de la organización.

La premisa fundamental de esta empresa es la eficiencia en cada una de las acciones que realiza, con miras a lograr la excelencia en sus servicios asumiendo, como prerrequisito, la calidad personal, la que conlleva al compromiso de cada miembro de la organización, aportando lo mejor de sí.

La empresa ha trabajado en definir su Misión y Visión a partir de la inauguración del nuevo edificio propio en el 2007, de la siguiente forma:

Misión

Ser líderes en el asesoramiento de las personas y las empresas, para la protección de la vida y su patrimonio. Todo esto mediante un adecuado asesoramiento dentro de los principios de ética.

Visión

Satisfacer las necesidades en el mercado, llegando a las personas y a las empresas a través de una fuerza de venta capacitada y profesional, con productos adecuados a cada necesidad y brindando beneficios tangibles, por la pertenencia a un grupo de afinidad.

La empresa estableció, también, los objetivos estratégicos de la misma:

- Mejorar la eficiencia y productividad en el quehacer permanente de la empresa.
- Mejorar la posición competitiva de la empresa en el ámbito regional.
- Mejorar la atención de los clientes, reduciendo los tiempos de espera en la tramitación y otorgamiento de beneficios.
- Obtener información confiable y útil para la toma de decisiones en materia de crecimiento y asesoramiento en protección de la vida y su patrimonio.
- Administrar los riesgos asociados al activo (la información) de la empresa.
- Cumplimiento de políticas internas con respecto al resguardo de la información.

II.3.2.1 Estructura vigente en la empresa

El modelo elegido por la empresa es una estructura funcional (Figura II.8 Estructura funcional de la empresa). Este modelo reúne, en un departamento, a todos los que se dedican a una actividad o a varias relacionadas, que se llaman funciones.

Generalmente este modelo lo usan pequeñas empresas que ofrecen una línea limitada de productos, porque aprovecha con eficiencia los recursos especializados. La estructura funcional facilita el movimiento de las habilidades especializadas, para poder usarlas en los puntos donde más se necesitan.

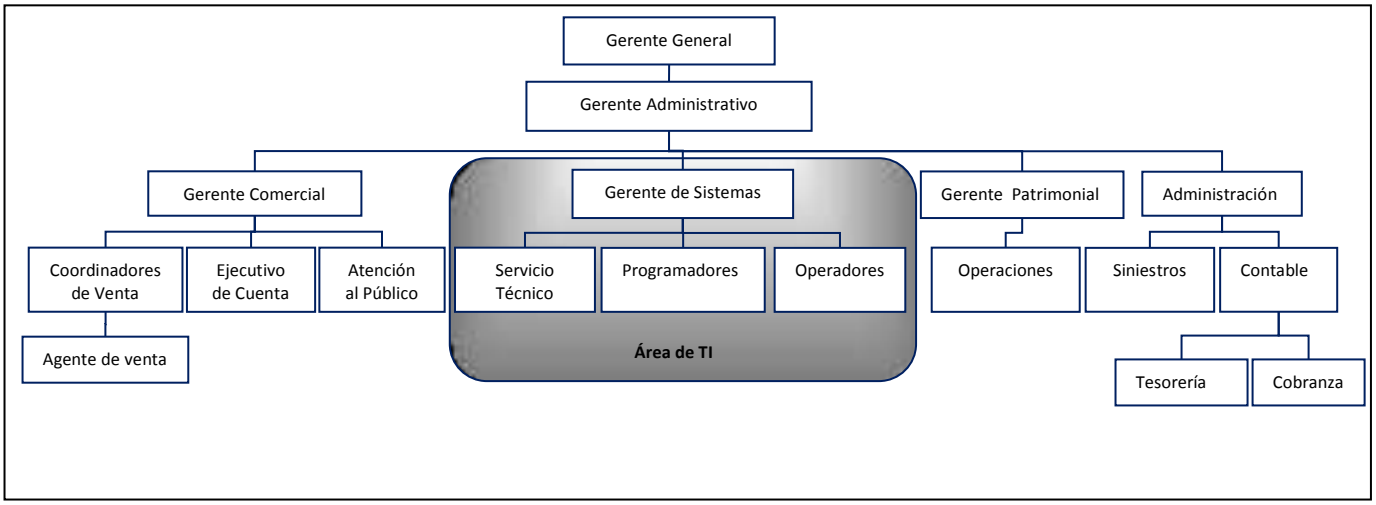


Figura II.8 Estructura funcional de la empresa

II.3.2.2 Área de TI

Se refiere a la unidad dentro de una organización que suministra – o coordina el uso de – diversos servicios de tratamiento de la información. El término concreto utilizado para identificar a esta unidad varía de una organización a otra. [5]

El Área de TI ha declarado como objetivos de TI a los siguientes:

- Proteger y responder por todos los activos de TI.
- Reducir defectos y tareas repetidas en las soluciones y en la prestación de servicios.
- Mantener la integridad de la información y de la infraestructura de procesamiento.
- Garantizar que la información crítica y confidencial sea resguardada solo para aquello con acceso permitido.
- Garantizar que se pueda confiar en las transacciones de negocio y en los intercambios de información automatizados.
- Garantizar que los servicios y la infraestructura de TI puedan resistir y recuperarse de fallas debido a errores, ataques deliberados y desastres.

El Área de TI de la empresa de servicio tiene como función básica la administración de redes y de los sistemas de la empresa de seguro, de modo de garantizar el adecuado funcionamiento de estos y la atención de las necesidades operacionales, incluido el soporte funcional de los usuarios. El área de TI actualmente incluye las funciones de Servicio Técnico, los Programadores y los Operadores.

Actualmente el Área de TI realiza las siguientes funciones:

- Instalación y configuración de equipos.
- Altas y bajas de usuarios.
- Instalación y configuración de aplicaciones.
- Mantenimiento de equipos de usuarios.
- Copias de seguridad de los datos de los usuarios
- Desarrollo de nuevas aplicaciones según las necesidades del Área de TI o de la empresa de seguro.
- Administrar y mantener la disponibilidad y funcionamiento de los servidores (hardware y software).

II.3.2.3 Tecnología

Debido al traslado al nuevo edificio, la empresa modernizó el equipamiento de hardware desde las estaciones de trabajo hasta los servidores. La adquisición de este moderno equipamiento fue realizada para que sea acorde a la situación estética del nuevo edificio.

Por lo tanto, la empresa cuenta con computadoras modernas, acceso a **Internet** de alta velocidad, redes informáticas internas y equipos multifunción para estar en condiciones de competir con éxito en el mercado, más allá de las características propias de sus productos o servicios. Los recursos tecnológicos que cuenta ayudan a desarrollar las **operaciones cotidianas** de la empresa, así también a la toma de decisiones de la alta gerencia.

Su infraestructura cuenta con computadoras con plataformas Pentium, Pentium II, III e IV, con sistemas operativos Windows XP; y un servidor con sistema operativo Windows XP.

En la Tabla II.4 Sistemas de Información describe los sistemas que cuenta la empresa en la actualidad:

Tabla II.4 Sistemas de Información

Nombre Sistema	Descripción	Fecha de Creación	Responsables	Desarrollo
ORG. SEGUROS	Registra las Altas, Bajas de productos de seguros de afiliados y el seguimiento de los siniestros.	2004	Área Sistemas	Desarrollo a medida
ACCOUNT	Registra las operaciones contables de la organización.	2008	Área Contable	Es un paquete que tiene soporte que realiza algunas modificaciones a medida
NACIÓN	Registra las Altas, Bajas de productos de Capital de $50.000 y $100.000 seguros del Banco Nación	2008	Área Sistemas	Desarrollo a medida
PATRIMONIAL	Registra las Altas, Bajas de productos de seguros patrimoniales de la Provincia y el seguimiento de los siniestros de los mismos	2008	Área Patrimonial	Paquete
LIS	Lleva el control de todos los seguros para ser presentados al organismo que regula los seguros	2008	Área Contable	Paquete
PANEL DE CONTROL	Lleva el control únicamente de los seguros de Sepelio y vida cargados en el sistema Org. Seguros y Nación	2009	Gerencia	Desarrollo a medida

II.3.2.4 Diagnostico del Área de TI

Como primer diagnóstico en el Área de TI, se puede determinar que la misma no es considerada como un área estratégica para el apoyo del cumplimiento de los objetivos de la empresa, puesto que:

- No existe una planificación para adquirir TI en la empresa. Una prueba de ello es que no se realizó un estudio previo para la instalación del cableado estructurado, pasando por alto un aspecto importante como es la cantidad de estaciones necesarias para cada área de negocio ni mucho menos se planteó un crecimiento futuro de la empresa.

- Cuenta con procesos que se llevan de manera empírica, basada en la experiencia. Por ejemplo los criterios de seguridad de información que se aplican no se encuentran formalizados.
- No se registran las necesidades de cambios en los sistemas planteadas por los usuarios internos de la empresa.
- Con respecto a la utilización del software necesario, como ser el Sistema operativo y utilitarios, la empresa tiene instaladas versiones ilegales, esta nunca se planteó la adquisición de este software según las necesidades de la misma.
- No existen normas generales escritas para el personal de sistemas en lo que se refiere a sus funciones, ni procedimientos definidos a la seguridad de información ante eventuales fallas del hardware y software.
- El personal del Área no recibe capacitación planificada por parte de la empresa, es decir, la empresa no ve las necesidades del Área como estrategia orientada al negocio.
- Pérdida de información por una gestión inadecuada de los archivos de datos.

CAPÍTULO III

METODOLOGÍA DE GOBERNABILIDAD DE RECURSOS DE TI

En este capítulo se presenta una estrategia metodológica que permite a las empresas aplicar la gobernabilidad de sus recursos de TI. Se muestran aspectos, como la descripción de las fases de la estrategia metodológica, las técnicas e instrumentos que son utilizados para llevarla a cabo.

III.1 Introducción a la Metodología

Con la intención de tener una estrategia metodológica de trabajo que permita a las empresas lograr la gobernabilidad de sus recursos de TI, se propone en este capítulo una estrategia de trabajo organizado en fases y actividades.

Esta propuesta de trabajo surge a partir de que las pequeñas y medianas empresas del medio no disponen de una herramienta que permita organizar las actividades necesarias para poder encausar la gobernabilidad de sus recursos de TI; y poder vincular los requerimientos de negocios en relación con la información que se almacena, genera y disponen en el contexto de las mismas. Resulta entonces, necesario primero evaluar los controles internos que se han diseñado para los recursos de TI y de esta manera otorgar una garantía razonable a la información empresarial.

A partir de estas consideraciones, surge la posibilidad de relacionar la Auditoria Informática con la gobernabilidad de los recursos de TI, tomando como bases las directrices y recomendaciones del estándar COBIT y la evaluación de los procesos de TI desde la mirada del CMMI, lo cual ha sido considerado en esta propuesta metodológica. Entonces luego de obtener los resultados de las evaluaciones de los controles internos, se estaría en condiciones de definir y proponer una estrategia que encause los objetivos de negocios con los objetivos de TI, asegurando, entonces, que las tecnologías informáticas constituyen una alternativa aceptable para permitir que las empresas alcances sus objetivos.

En la propuesta metodológica se combinan fases, actividades, técnicas e instrumentos que conforman una buena alternativa para organizar el trabajo de gobernabilidad. En la primera fase corresponde al Análisis y Estudio preliminar de la empresa; en la segunda fase se busca Identificar y Diagnosticar la madurez de los procesos de TI y finalmente la tercera fase corresponde a la Auditoria Informática la cual tiene como propósito evaluar los controles internos diseñados para los recursos de TI y emitir las recomendaciones necesarias para encaminar a la empresa hacia la Gobernabilidad de los recursos de TI.

En la Figura III.1 Metodología de Gobernabilidad de Recursos de TI se muestran la interacción y vinculación entre las fases y actividades de la propuesta.

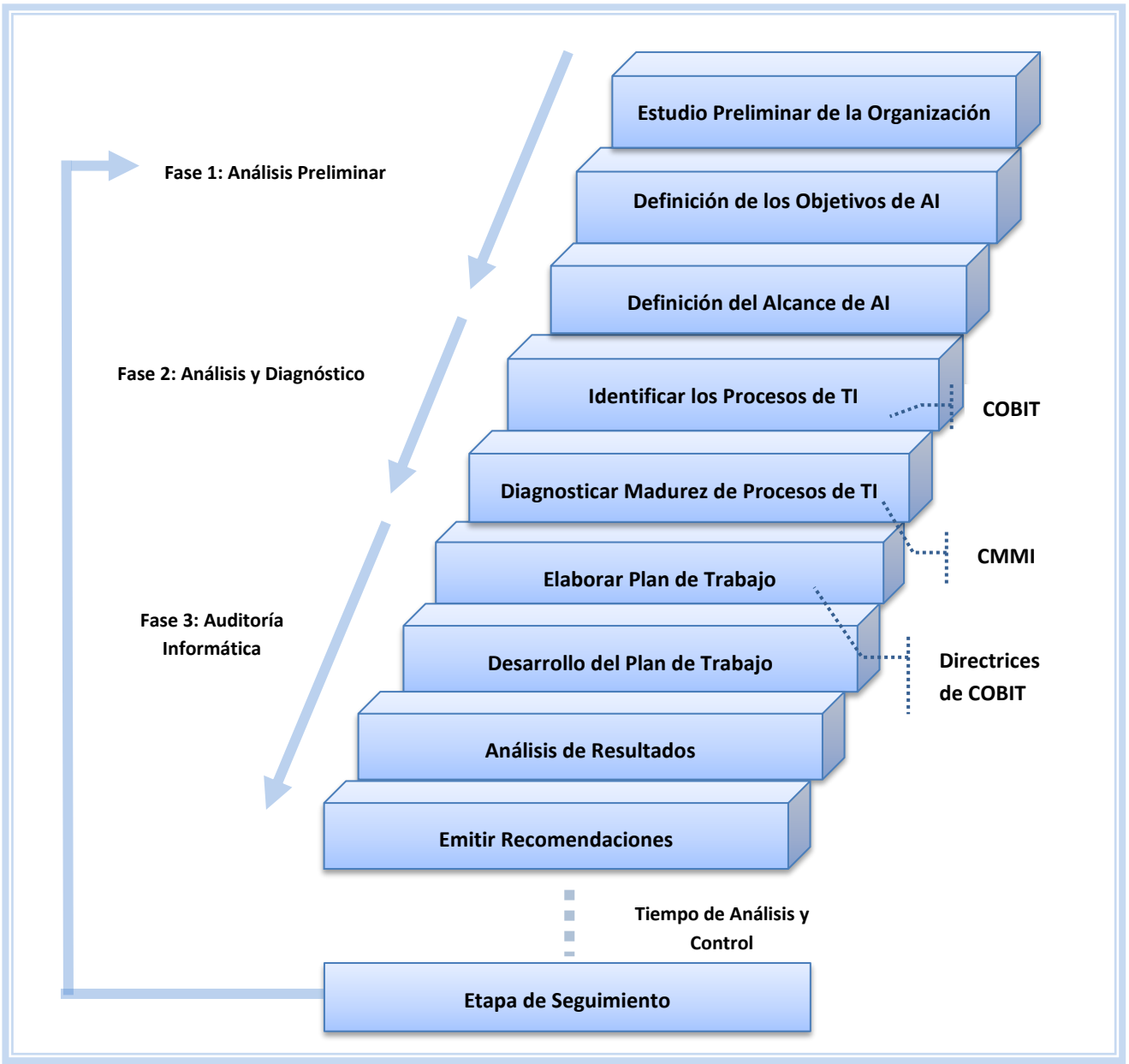


Figura III.1: Metodología de Gobernabilidad de Recursos de TI

III.2 DESCRIPCIÓN DE LA METODOLOGÍA

III.2.1 Fase 1. Análisis Preliminar

Durante esta primera etapa de la propuesta metodológica se busca un acercamiento a la organización, para comprender y clarificar la realidad y el contexto de trabajo de la AI, a

partir de esta visión general, se van a sustentar las bases para que la organización pueda encausar la gobernabilidad de sus recursos tecnológicos.

Las técnicas y herramientas que soportan las actividades de esta primera fase son las vinculadas con las técnicas de relevamiento, es decir la observación, entrevistas, análisis de registros, etc.

La empresa debe asignar un responsable interno, el cual debe poseer conocimientos técnicos y del negocio, pertinentes a las actividades por auditar. El responsable será quien acompañe al equipo externo en determinadas actividades de la auditoría y pondrá a disposición los medios necesarios para asegurar el desarrollo óptimo de la auditoría, y en un futuro, implementará las acciones correctivas, atendiendo al informe de la auditoría.
Durante esta fase resulta importante la identificación y clarificación de los objetivos de negocios y de los objetivos de TI que la empresa ha definido previamente. Resulta importante que se tengan en claro los objetivos de negocios, los cuales constituyen las guías de acción que ha definido la organización para su futuro inmediato, así también es necesario conocer cuáles son los objetivos de TI que se persiguen.

Establecer los objetivos de negocios es esencial para el éxito de una empresa, éstos establecen un curso a seguir y sirven como fuente de motivación para todos los miembros de la empresa.

Además, considerando que las organizaciones actuales hacen inversiones importantes en recursos de tecnología de información para apoyar los procesos de negocio, el valor significativo y relevante que el uso de la información tiene para las organizaciones, determina que todos los procesos relativos a la producción, administración y uso de servicios de TI deben ser óptimamente gestionados y controlados para asegurar la calidad de la información, soporte del cumplimiento de los objetivos del negocio.

Los procesos de datos e información producto de las operaciones y procesos del negocio, requieren la aplicación de técnicas y medidas de control en el marco de un sistema de gestión que garantice la prestación de los servicios y la reducción de amenazas que pongan en peligro la estabilidad de la organización. Todo esto, justifica la necesidad de optimizar los recursos de TI en apoyo y alineación con los objetivos de negocio a través de procesos efectivos de "gestión de servicio TI".

La definición de un conjunto de objetivos de negocio y de TI ofrece una base más refinada y relacionada con la organización para el establecimiento de requerimientos de negocio y para el desarrollo de métricas que permitan la medición con respecto a estos objetivos.

Si se pretende que las TI proporcione servicios de forma exitosa para dar soporte a la estrategia de la empresa, debe existir una dirección clara de los requerimientos por parte de la organización y un claro entendimiento para las TI.

Las actividades que involucra esta Fase Preliminar son:

- Estudio Preliminar de la Organización.
- Definición de los Objetivos de AI.
- Definición del Alcance de AI.

La primera actividad permite tomar contacto con la organización y su contexto, con el fin de tener una visión general de la misma para encauzar la gobernabilidad de los recursos informáticos, se pone especial énfasis en identificar y clarificar los objetivos de negocios y los objetivos de TI.

A partir de la actividad anterior, se definen los objetivos de la AI; el cual dependerá de donde pone énfasis la organización cuando define los objetivos de negocio y los objetivos de TI definidos.

Definido los objetivos, se establece el alcance de la AI, en donde se ha de definir con precisión el entorno y los límites en que va a desarrollarse esta tarea, se complementa con los objetivos de ésta. El alcance ha de figurar expresamente en el informe final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino también que se ha omitido. La indefinición de los alcances de la auditoría compromete el éxito de la misma.

Los resultados que se obtienen de esta primera Fase son:

- Identificación de Objetivos de Negocios.
- Identificación de Objetivos de TI.
- Objetivos generales de Auditoria Informática.
- Alcance de la Auditoria Informática.

En la Figura III.2 Estudio preliminar, se muestran las actividades y resultados de esta fase.

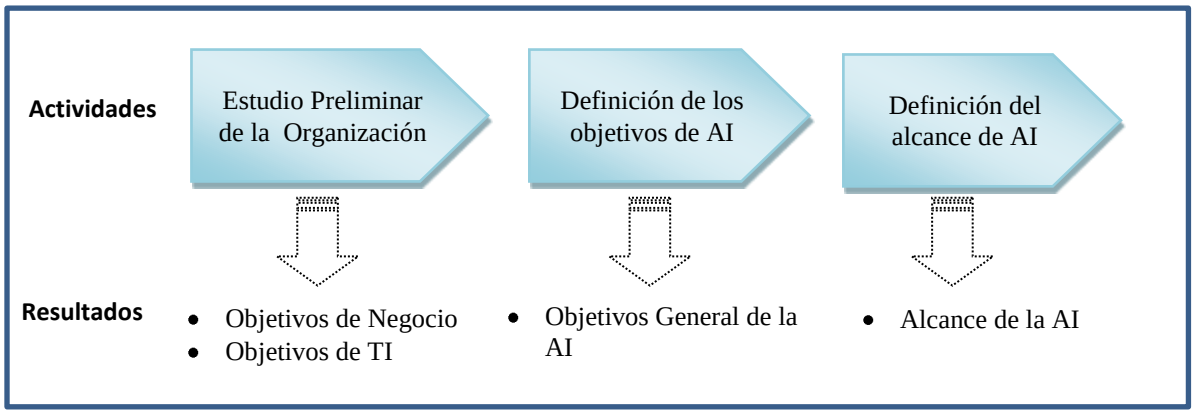


Figura III.2 Estudio Preliminar

III.2.2 Fase 2. Análisis y Diagnóstico

Planteado la base sobre el que se realizara la AI es necesario identificar el ámbito de la auditoria, esto es, establecer en la organización los procesos de TI que se van a auditar.

Los servicios de TI se deben poner a disposición para que se cumplan las expectativas de la organización de forma efectiva y eficiente. Esto es llevado a cabo mediante la combinación adecuada de personas, procesos y tecnología de la información, los cuales constituyen los Procesos de TI.

Entonces para tener una idea clara de lo que se persigue en esta fase y tener una aproximación sobre la realidad de los Procesos de TI en la organización y poderlos encaminar hacia su gobernabilidad, resulta conveniente que se identifiquen los procesos de TI vinculados con los objetivos de Auditoria, y luego evaluarlos sobre su estado de madurez.

Como herramientas de soporte de esta fase se recurre al estándar COBIT el que constituye una herramienta que define las actividades de TI en un modelo de treinta y cuatro procesos genéricos agrupados en cuatro dominios, los cuales han sido presentado en el capítulo II.

Además, también, se utiliza el Modelo CMMI, este es un modelo de evaluación de los procesos de una organización, que también ha sido presentado en el capítulo II.

Las actividades que involucran esta Fase Análisis y Diagnóstico son dos:

- Identificar Procesos de TI.
- Diagnosticar Madurez de Procesos de TI.

Para **Identificar los Procesos de TI** se llevan a cabo las siguientes acciones, según lo establece el estándar COBIT:

1- Identificar los Criterios de Información: Se identifican los criterios de Información a evaluar, teniendo en cuenta los objetivos de AI establecidos en la fase anterior.

2- Seleccionar los Procesos de TI: Se vinculan los Procesos de TI a los criterios de Información seleccionados anteriormente, a partir de una propuesta realizada por el estándar COBIT. Se seleccionan los Procesos de TI relevantes que tenga un impacto primario (P) con los criterios de información relacionados, teniendo como referencia el tamaño y características de la organización.

Para **Diagnosticar el Nivel de Madurez** de los Procesos de TI seleccionados se propone realizar las siguientes acciones:

1- Estudiar los Procesos de TI: Según el modelo de Madurez CMMI, se han definido seis niveles en el que es posible que se encuentre, en este caso, un Proceso de TI que se está evaluando. Estos niveles, según lo planteado en el Marco Conceptual, son:

0- No Existente
1- Inicial
2 - Repetible
3 - Definido
4 - Administrado
5 - Optimizado

Al finalizar esta actividad se completa la Tabla III.1 Condiciones Significativas de Procesos de TI, donde se estudia las condiciones significativas que deben cumplir los Procesos de TI para cada uno de los niveles del modelo de CMMI.

Tabla III.1 Condiciones Significativas de Procesos de TI

Procesos de TI	Madurez de Procesos de TI					
	No Existente	Inicial	Repetible	Definido	Administrado	Optimizado
Proceso 1						
Proceso 2						
…						
Proceso x						

Condiciones significativas del Proceso 1 para el Nivel No Existente.

2- Seleccionar Parámetros para evaluar los Procesos de TI: En esta actividad se identifican y seleccionan los parámetros que servirán para facilitar la evaluación de los Proceso de TI por parte de los evaluadores. La selección de los parámetros la debe realizar el auditor teniendo en cuanta las características de la organización bajo estudio, los objetivos de AI y las condiciones significativas de los Procesos de TI para cada nivel de Madurez de la tabla obtenida de la acción anterior.

Al finalizar esta actividad se construye la Tabla III.2 Condiciones Significativas de Parámetros, en la cual se describen las condiciones de cada parámetro seleccionado, según los distintos niveles que pueden alcanzar, la cual ayudará en la aplicación del modelo matemático que se desarrolla en la siguiente acción: Evaluar Procesos.

Tabla III.2 Condiciones Significativas de Parámetros

Nivel	Parámetros			
	Parámetro 1	Parámetro 2	…	Parámetro N
No Existente				
Inicial				
….				
Optimizado				

Condiciones significativas del Parámetro 1 para el Nivel No Existente.

3- Evaluar Procesos de TI: Esta actividad tiene como finalidad evaluar los procesos de TI seleccionados en la actividad anterior, a partir de información relevada de la organización, se puede recurrir a técnicas de recolección de datos como encuestas estructuradas, entrevistas, entre otras.

En esta actividad se debe realizar acciones como:

- **Identificación de la Muestra:** Para la selección de la muestra se elige un subconjunto de la población representativo para la evaluación de los Procesos de TI.
- **Construcción de la Hoja de Evaluación y Aplicación del Modelo Matemático:** Para evaluar el estado de madurez del proceso de TI, se propone la contrucción de una hoja de evaluación para que los evaluadores del Proceso puedan realizar rápida y globalmente una evaluación de los parámetros de los Procesos de TI.

  En este Trabajo academico, también se propone un modelo matemático a seguir, quien establecerá el nivel de madurez que se encuentra el proceso de TI, con el fin

de priorizar los requisitos y directrices que deben ser mejorados y establecer políticas y directrices encaminadas a mejorar el nivel de madurez.

Para valorar cada parámetro se ha asignado una puntuación comprendida entre cero y cinco de acuerdo a los criterios establecidos en la descripción del nivel de madurez.

La muestra seleccionada debe realizar, como primera instancia, la lectura de las caracteristicas de los niveles de Madurez para cada parametro del proceso evaluado.

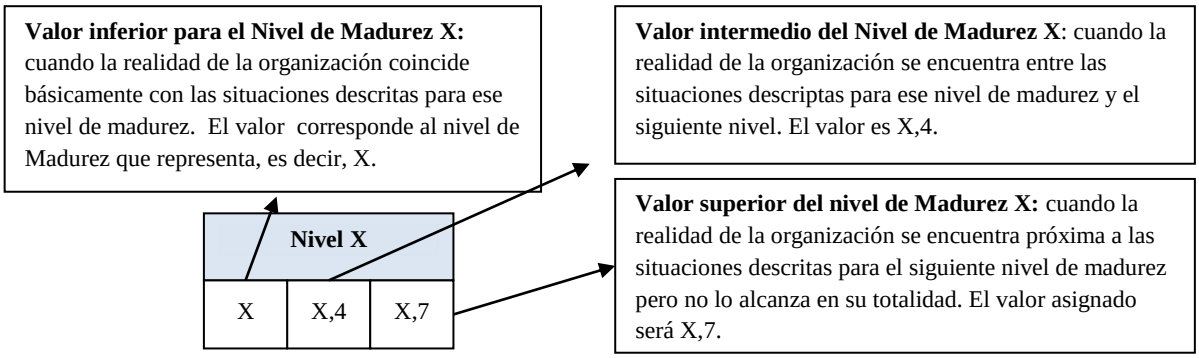
No se debe puntuar un nivel como alcanzado si no se cumplen totalmente los criterios de evaluación asignados para ese nivel.

En el diseño de la hoja de evaluación se incorpora el modelo matemático que determina el nivel de madurez del Proceso de TI. A continuación la Tabla III.3 Hoja de Evaluación muestra el diseño para realizar la evaluación del proceso.

Tabla III.3 Hoja de Evaluación

Proceso: XXXXXX																		
Parámetros	**Niveles de Madurez**																	
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No Existente			**Inicial**			**Repetible**			**Definido**			**Administrado**			**Optimizado**		
Parámetro 1																		
Parámetro 2																		
…																		
Parámetro n																		

Cada uno de estos valores está subdivido en tres casillas para que la muestra seleccionada opte por uno de ellos. Por ejemplo para un nivel X a considerar:



Se selecciona el nivel de madurez que más se aproxime a la realidad de la empresa y se anota dicho valor según corresponda, mediante una cruz. En la Tabla III.4 Ejemplo de

Hoja de Evaluación la referencia A indica que el evaluador marco la primera casilla del Nivel 2 para el parámetro 1 del proceso evaluado.

Tabla III.4 Ejemplo de Hoja de Evaluación

Proceso: XXXXXX																		
Parámetro	**Nivel de Madurez**																	
	0			**1**			**2**			**3**			**4**			**5**		
	No Existente			**Inicial**			**Repetible**			**Definido**			**Administrado**			**Optimizado**		
Parámetro 1							X											
Parámetro 2					X													
…							X											
…								X										
Parámetro n								X										

Tabla III.5 Evaluación del Proceso

Número de Casillas Puntuadas	0	0	0	0	1	0	2	2	0	0	0	0	0	0	0	0	0	0
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5		
Puntos Obtenidos por cada Columna (n° de casillas x valor)	0			0	1,4	0	4	4,8	0	0	0	0	0	0	0	0		
Resultado Final= Suma de todas las columna dividido 5																2,04		

Para obtener el resultado final (**E**), como muestra la Tabla III.5 Evaluación del Proceso, se calcula la media aritmética de la suma de los puntos obtenidos. Para ello:

1. Se registra el número de casillas puntuadas en cada columna (**B**)

2. Se calculan los puntos obtenidos por cada columna (**D=B x C**), multiplicando el número de casillas puntuadas (**B**), por el valor asignado a cada casilla (**C**).

3. Se suma el total de puntos obtenidos por cada columna (**D**), y se calcula su media aritmética dividiendo el total entre 5 (número de atributos evaluados), lo que da el resultado final (**E**).

El nivel de Madurez para un Procesos de TI se determina realizando el promedio de todos los resultados de las Hojas de evaluación realizadas.

Nivel de Madurez = $\sum$ (Ei)/NHE

NHE: Número de Hoja de Evaluación.

Ei: Es el resultado final obtenido para el Proceso i de cada Hoja de evaluación.

4- Análisis de Resultados: En esta etapa se analiza el valor obtenido a partir del modelo matemático seleccionado en la etapa anterior, que determina el estado de madurez del proceso de TI evaluado.

Los resultados que se obtienen de esta segunda Fase son:

- Procesos de TI vinculados con los objetivos de TI.
- Nivel de madurez de los Procesos de TI seleccionados.

En la Figura III.3 Análisis y Diagnóstico, se muestran las actividades y resultados de esta fase.

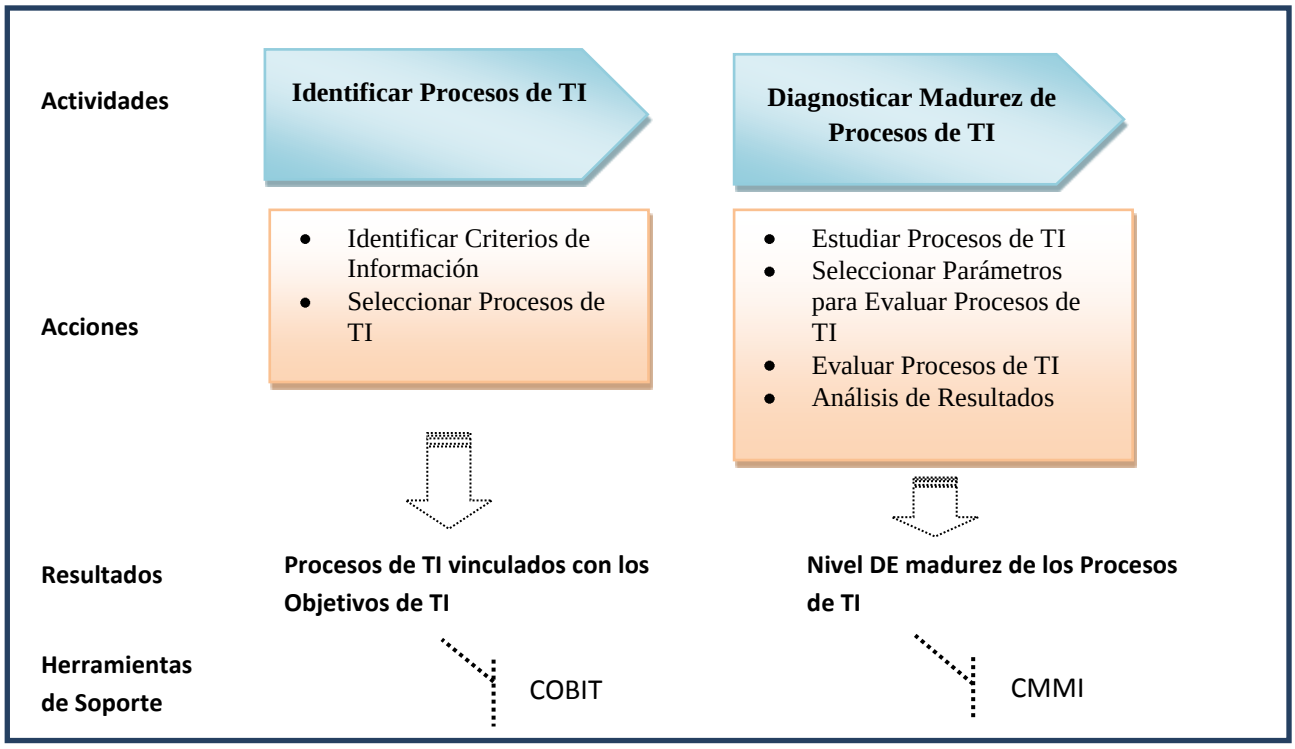


Figura III.3 Análisis y Diagnóstico

III.2.3 Fase 3: Auditoría Informática

Considerando que la AI tiene como función verificar y asegurar que las políticas y procedimientos establecidos para el manejo y uso de la tecnología informática en la organización se realicen de manera eficiente y eficaz, las actividades que proponemos para esta fase son:

- Elaborar Plan de Trabajo

- Desarrollo del Plan de Trabajo
- Emitir Recomendaciones

El Plan de Trabajo ayuda en la implementación de las buenas prácticas de trabajo que hacen falta y define una trayectoria de evaluación que permitirá dar seguimiento y continuidad al proceso de mejora continua.

La Tabla III.6 Plan de trabajo, esquematiza para cada uno de los Procesos de TI los objetivos de control que serán evaluados.

Tabla III.6 Plan de Trabajo

Plan de Trabajo				
Objetivo:				**Duración**
Actividades:				
Proceso	**Documentos a evaluar**	**Controles a evaluar**	**Objetivo de TI que satisface**	**Objetivo de negocio que satisface**

Los campos que se utilizan se describen a continuación:

- **Objetivo**: Indicar el objetivo o finalidad del plan de Trabajo, que dependerá del objetivo de la AI.
- **Actividades**: Es el listado de las actividades que deben ser implementadas para evaluar los controles internos.
- **Proceso:** Nombre del proceso de TI a evaluar.
- **Documentos a evaluar:** Listado de documentos que serán analizados para evaluar proceso de TI.
- **Controles a evaluar**: Son tareas específicas que se deben realizar para alcanzar el control del proceso. Los controles a evaluar se seleccionan de las Directrices del estándar COBIT teniendo como referencia las carácterísticas organizacionales de la empresa, como así también las condiciones de cada Proceso de TI, según el Nivel de Madurez obtenido en la fase anterior.
- **Objetivo de TI que Satisface:** Objetivo de TI de la organización que satisface el proceso de TI.

- **Objetivo de Negocio que Satisface**: Descripción de cómo el objetivo de control se enlaza con los objetivos y requerimientos de negocio.

En el **Desarrollo del Plan de Trabajo,** se efectivizan las actividades planificadas, aplicando distintas técnicas y utilizando herramientas que garanticen el cumplimiento de los objetivos planteados.

Para auditar cada Proceso de TI se recurren a distintas técnicas de relevamiento las que permitirán que el auditor pueda tener evidencias necesarias para elaborar su opinión que se informará finalmente.

Para el **Análisis de Resultados** a partir del relevamiento, se analizarán si los controles evaluados para cada Procesos de TI propuestos por COBIT existen y la forma que son implementados en la empresa, determinando las debilidades para cada Proceso de TI evaluado.

En la actividad **Emitir Recomendaciones** se describen las recomendaciones, las cuales están basadas en el análisis de las Directrices del estándar COBIT y los resultados obtenidos en la actividad Desarrollo del Plan de Trabajo.

Los resultados que se obtienen de esta tercera Fase son:

- Plan de Trabajo.
- Entrevistas, cuestionarios y análisis de resultados.
- Recomendaciones.

En la Figura III.4 Auditoria Informática, se muestran las actividades y resultados de esta fase.

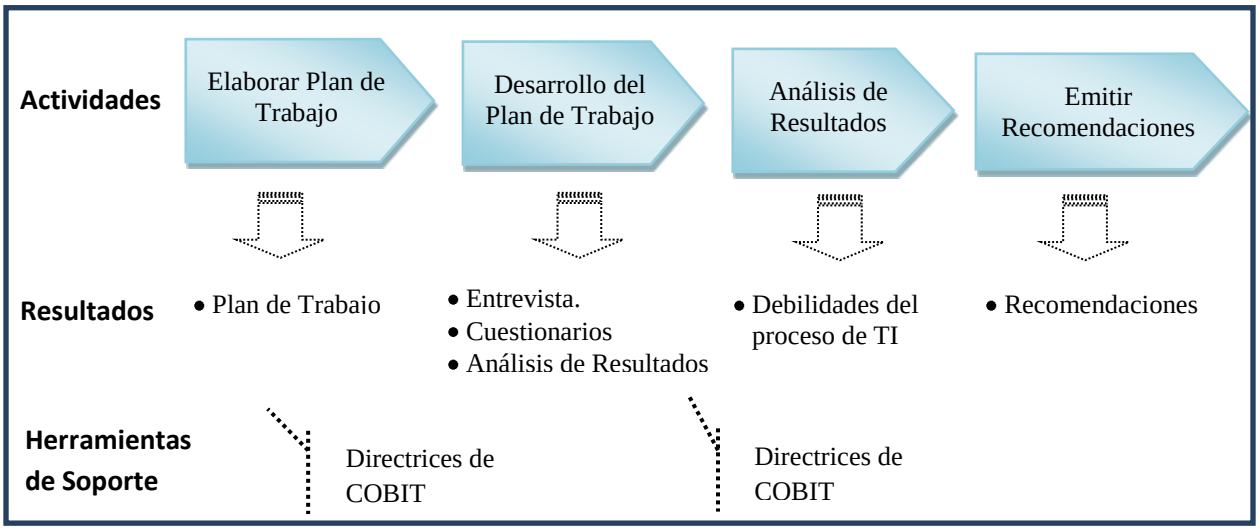


Figura III.4 Auditoría Informática

III.2.4 Etapa de Seguimiento

Esta etapa consiste en el seguimiento y control por parte de la empresa para llevar a cabo las recomendaciones propuestas en la AI.

Se propone elaborar el seguimiento de las recomendaciones propuestas en la AI, el cual consiste en establecer procedimientos de control para el monitoreo de la implementación de las recomendaciones para cada proceso de TI auditado.

Para ello es preciso mantener un registro formal y consolidado de las características relevantes de las recomendaciones de cada proceso de TI, que permita contar con información actualizada y tomar medidas adecuadas en el caso que ocurran desviaciones.

Se recomienda, para llevar a cabo esta etapa, nombrar un equipo de implementación formado por directivos, gerentes de áreas y coordinados por el responsable interno nombrado en las primeras etapas. Aunque, la conformación del equipo de implementación puede diferir con la propuesta dependiendo de diversas características que posee una empresa, por ejemplo, su tamaño, distribución geográfica, tipo de organización, etc.

En esta etapa los responsables de cada proceso de TI deben presentar los resultados de la aplicación del seguimiento al equipo de implementación cada cierto periodo de tiempo y realizar un análisis de las desviaciones ocurridas respecto a lo planificado.

Para ello, se elabora un plan de seguimiento y control, el cual define las actividades a realizar para controlar la ejecución de las recomendaciones realizadas en la AI.

Se sugiere presentar la información del seguimiento como muestra Tabla III.7 Seguimiento y Control con la siguiente estructura:

Tabla III.7 Seguimiento y Control

Nombre del Proceso de TI				
Mecanismo de control				
Frecuencia				
Control	**Requisito de Aceptación**	**Indicador de Seguimiento**	**Desviación**	**Responsable**
Hito 1				
Hito 2				
…				
Hito N				

A continuación se detalla cada ítem de la plantilla:

- **Nombre del Proceso de TI**: Nombre del Proceso de TI que se realiza el seguimiento y control.
- **Mecanismos de control**: Consisten en la definición y explicación de los procedimientos mediante los cuales se llevará a cabo el control.
- **Frecuencia**: Número de veces que se realiza el control al Proceso de TI durante un período de tiempo.
- **Hitos de control**: Los hitos de control corresponden a actividades que determinan el término de un conjunto de etapas para llevar a cabo recomendaciones realizadas en la AI.
- **Requisitos de aceptación**: Los requisitos para la aceptación conforme de cada hito de control, corresponden al resultado esperado que determina la satisfacción del cumplimiento de un hito.
- **Indicadores de seguimiento**: Corresponden a las variables que permitirán monitorear el alcance del hito de control y el uso de los recursos, a medida que se van efectuando los controles.
- **Desviación**: Es la diferencia entre el Requisito de Aceptación con el Indicador de Seguimiento, o una Observación cualitativa del Hito de Control observado.
- **Responsables de los hitos de control**: se debe especificar los responsables para el control de los hitos.

En un periodo de seis meses, se realiza un estudio de los resultados de la tabla de seguimiento donde son analizadas las desviaciones ocurridas respecto a lo planificado, para hacer las correcciones necesarias. Las desviaciones serán analizadas por el responsable del proceso de TI, quien tomará las medidas necesaria dependiendo el tipo de desviación o hito de control en el cual ocurrió.

Se recomienda que luego de dos años, se realice una nueva autoevaluación de la madurez de los Procesos de TI, volviendo a la Fase 1 de la Metodología de Gobernabilidad, entendiendo que el proceso de maduración del Gobierno de las TI es un proceso de mejora continua.

Cabe señalar que el plan de seguimiento incorpora los aspectos mínimos a considerar para su aplicación, ya que puede ser enriquecida con elementos adicionales a los presentados en esta tesis, quedando a consideración del equipo de implementación. Así también, los

periodos de análisis de control de los Procesos de TI y Autoevaluación de Madurez de los mismos, pueden ser modificados a criterio del mismo equipo.

CAPÍTULO IV

GOBERNABILIDAD DE LOS RECURSOS DE TI

GOBERNABILIDAD DE LOS RECURSOS DE TI

Este capítulo tiene como propósito llevar a cabo las etapas de la Metodología de Gobernabilidad de los Recursos de TI, que se ha definido en el Capítulo III, en una empresa de seguro de nuestro medio, con el fin de encaminarla hacia el Gobierno de TI.

IV.1 DESARROLLO DE LA METODOLOGÍA DE GOBERNABILIDAD DE RECURSOS DE TI

La Metodología de Gobernabilidad de Recursos de TI, asiste a los responsables del trabajo a implementar el Gobierno de TI en una empresa del medio identificando que Procesos de TI deben ser mejorados. La empresa seleccionada es una aseguradora, cuya necesidad es de contar con un marco de trabajo de buenas prácticas que le permita alinear los objetivos del negocio, administrar sus recursos y optimizar la prestación de los servicios.

A continuación se desarrollan cada una de las fases de la Metodología de Gobernabilidad de Recursos de TI:

IV.1.1 Fase 1: Análisis Preliminar

IV.1.1.1 Estudio Preliminar de la Organización

En esta fase preliminar, se inicia tomando contacto con la organización y su contexto, con el fin de tener una visión general en donde se va a trabajar, para encauzar la gobernabilidad de sus recursos informáticos; en el caso particular de este trabajo, este análisis del contexto organizacional se realizó en el capítulo anterior, en el Marco Empírico.

En esta fase también se designa al Gerente de Sistema como responsable interno de la empresa, para que acompañe al equipo externo a lo largo de la metodología, con el fin de que realice las acciones correctivas en la etapa de seguimiento de la metodología.

La empresa ha tenido un desarrollo importante en el área de TI en los últimos años para acompañar el crecimiento del negocio, incrementando su dependencia en TI para hacer más eficientes sus procesos y alcanzar sus objetivos de negocio. Esta dependencia del negocio sobre las TI, conduce a la necesidad de:

- Minimizar el riesgo de eventos no deseados que afecten los servicios informáticos. Dichos eventos deben ser prevenidos, detectados y corregidos, por lo que es necesario establecer mecanismos de control para la seguridad de la información.
- Uso eficiente de la información y su protección.

A continuación se expresan los siguientes objetivos de negocio estratégicos definidos por la empresa:

- Mejorar la eficiencia y productividad en el quehacer permanente de la empresa.
- Mejorar la posición competitiva de la empresa en el ámbito regional.
- Mejorar la atención de los clientes, reduciendo los tiempos de espera en la tramitación y otorgamiento de beneficios.
- Obtener información confiable y útil para la toma de decisiones en materia de crecimiento y asesoramiento en protección de la vida y su patrimonio.
- Administrar los riesgos asociados al activo (la información) de la empresa.
- Cumplimiento de políticas internas con respecto al resguardo de la información.

Relacionados con estos, la organización también ha declarado como objetivo de TI a los siguientes:

- Proteger y responder por todos los activos de TI.
- Reducir defectos y tareas repetidas en las soluciones y en la prestación de servicios.
- Mantener la integridad de la información y de la infraestructura de procesamiento.
- Garantizar que la información crítica y confidencial sea resguardada solo para aquello con acceso permitido.
- Garantizar que se pueda confiar en las transacciones de negocio y en los intercambios de información automatizados.
- Garantizar que los servicios y la infraestructura de TI puedan resistir y recuperarse de fallas debido a errores, ataques deliberados y desastres.

Para el análisis de los objetivos planteados anteriormente, nos centramos en la definición de alineación objetivos, una de las actividades principales del GTI, el cual señala que si los objetivos de TI sustentan a los objetivos de la empresa se crea la capacidad necesaria para crear valor en la misma; esto implica que las operaciones de las TI den respuestas a las operaciones de la empresa.

Teniendo en cuenta la definición anterior, para alcanzar la alineación, se analizan los objetivos de TI y los objetivos estratégicos de la empresa para verificar si desde el punto de

vista estratégico las TI están contempladas por la alta gerencia para alcanzar los objetivos de negocio.

Se puede verificar que formalmente los objetivos de TI dan sustento a los objetivos estratégicos de la empresa, es decir, que ambos objetivos están en armonía para el logro de los objetivos de negocio.

Según la definición plateada en un comienzo, esta alineación existente desde lo formal de los objetivos de TI y de los objetivos estratégicos de la empresa, implica que las operaciones de TI están dando respuestas a las operaciones de la empresa, lo cual se verificaría través de una AI, que evalúe los controles de los Procesos de TI estudiados.

En la Tabla IV.1 Relación entre objetivos Estratégicos de la Empresa con Objetivos de TI, muestra la correlación entre ambos objetivos quedando demostrada esta afirmación.

Tabla IV.1 Relación entre Objetivos Estratégicos de la Empresa con Objetivos de TI

Objetivos Estratégicos de la Empresa	Objetivos de TI
• Mejorar la atención de los clientes, reduciendo los tiempos de espera en la tramitación y otorgamiento de beneficios.	• Reducir defectos y tareas repetidas en las soluciones y en la prestación de servicios.
• Obtener información confiable y útil para la toma de decisiones en materia de crecimiento y asesoramiento en protección de la vida y su patrimonio.	• Garantizar que se pueda confiar en las transacciones de negocio y en los intercambios de información automatizados.
• Administrar los riesgos asociados al activo (la información) de la empresa.	• Proteger y responder por todos los activos de TI.
	• Mantener la integridad de la información y de la infraestructura de procesamiento.
• Cumplimiento de políticas internas con respecto al resguardo de la información.	• Garantizar que la información crítica y confidencial sea resguardada solo para aquello con acceso permitido.

Para el desarrollo de la AI se toma como referentes los objetivos de negocio estratégicos definidos por la empresa y los de objetivos de TI, de los cuales se desprende la importancia de la seguridad de la información, cuyo reto es tener la capacidad de lograr todos los objetivos antes mencionados, para que así, la organización pueda tener un desempeño óptimo basado en un buen estado de su infraestructura informática, que en estos tiempos es vital para todos los tipos de asociaciones.

IV.1.1.2 Definición de los Objetivos de AI

A partir de este planteo organizacional se expresan los siguientes objetivos generales para la AI:

- *Evaluar que los recursos de TI de la empresa se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.*
- *Asegurar a la alta dirección y al resto de las áreas de la empresa que la información sea precisa y suficiente y que les llega en el momento oportuno, para tomar decisiones importantes.*
- *Asegurar la protección de la información sensible contra divulgación no autorizada.*

Del cual se desprenden los **objetivos específicos**:

- *Identificar los procesos de TI asociados a la seguridad de la información.*
- *Diagnosticar los procesos de TI a través del Modelo de Madurez Integrado (CMMI).*
- *Evaluar la eficiencia y eficacia de los Procesos de TI.*
- *Proporcionar a la Alta Dirección información del estado de los Procesos de TI y el resultado de aplicar la AI.*

IV.1.1.3 Definición del Alcance de AI

Una vez establecidos los objetivos de la AI, se define el alcance de la misma, determinando que la AI se llevará a cabo en el Área de TI, específicamente en los Procesos de TI donde la eficacia y eficiencia impactan en forma directa en la seguridad de la información de la empresa.

IV.1.2 Fase 2: Análisis y Diagnostico

Con la intención de tener una definición clara sobre el ámbito en donde se realizará la AI, en esta fase se identifican, como se indicó en la metodología propuesta, los Procesos de TI que estén vinculados con los objetivos definidos para la AI.

Para poder llevar a cabo esta fase, se llevan a cabo dos actividades:

IV.1.2.1 Identificar los Procesos de TI

En la identificación de los Procesos de TI se llevan a cabo las siguientes acciones, recurriendo a los principios del estándar COBIT:

IV.1.2.1.1 Identificar los Criterios de Información.

Para la identificación de los Procesos de TI se tendrá en cuenta los criterios de información relacionados al requerimiento de negocio **seguridad de la información**, ya que en la fase anterior se hizo mención a la misma como prioridad a tener en cuenta para la empresa de seguro. Según el estándar COBIT los tres criterios de información que son utilizados a nivel mundial para describir los requerimientos de seguridad de la información son: **Confidencialidad, Integridad y Disponibilidad**.

IV.1.2.1.2 Seleccionar los Procesos de TI

Para seleccionar los procesos de TI se tiene en cuenta la tabla que propone el estándar COBIT que muestra una visión global de la relación entre los procesos de TI y los criterios de información (Anexo E: Tabla de Prioridad), la cual permite identificar aquellos criterios de información que tienen una relación primaria o secundaria sobre todos los Proceso de TI. Como los objetivos y alcance de la AI hacen referencia solo a procesos de TI no se tendrá en cuenta la relación entre los procesos con los recursos que se expresan en la Tabla de prioridad.

A partir de esta tabla, se pueden identificar todos los procesos de TI cuyos criterios de información relacionados a la seguridad de la información tienen un impacto Primario (P) y Secundario (S). Esto se ve reflejado en la Tabla IV.2 Relación de los Procesos de TI con los Criterios de Información, donde se filtran solo aquellos Procesos de TI relacionados con los criterios de Información **Confidencialidad, Integridad y Disponibilidad**.

Para este trabajo académico, la selección de los procesos de TI, se realiza teniendo como referencia el tamaño, las características de la empresa de seguro y los objetivos estratégicos de la organización. Se busca seleccionar aquellos procesos que tienen un mayor grado de significación con respecto a la seguridad de la información, cuestión que es crítica para el objetivo de auditoria que se ha fijado. Para ello se identifican aquellos procesos con dos o más impacto primario (P) sobre los criterios de información relacionados con la **seguridad de la información**, obteniéndose la Tabla IV.3 Procesos de TI de la empresa.

Además en esta tarea se contó con la asistencia del responsable interno de la empresa, el cual ha apoyado la selección realizada considerando que se trata de procesos de TI relevantes para las políticas futuras de la organización.

Por último, destacar que esta selección de procesos se lleva a cabo a partir de lo propuesto por el estándar COBIT.

Los Procesos de TI seleccionados son:

- Evaluar Riesgos
- Administrar Cambios
- Garantizar la Seguridad de Sistemas
- Administrar Instalaciones

Tabla IV.2 Relación de los Procesos de TI con los Criterios de Información

		Criterios de información						
Dominio	**Proceso**	Efectividad	Eficiencia	**Confidencialidad**	**Integridad**	**Disponibilidad**	Cumplimiento	Confiabilidad
Planeación y Organización								
PO2	Definir la Arquitectura de Información	P	S	**S**	**S**			
PO9	Evaluar Riesgos	S	S	**P**	**P**	**P**	S	S
PO11	Administrar Calidad	P	P		**P**			S
Adquisición e Implementación								
AI2	Adquisición y Mantener Software de Aplicación	P	P		**S**		S	S
AI3	Adquirir y Mantener Arquitectura de TI	P	P		**S**			
AI4	Desarrollar y Mantener Procedimientos relacionados con TI	P	P		**S**		S	S
AI5	Instalar y Acreditar Sistemas	P			**S**	**S**		
AI6	Administrar Cambios	P	P		**P**	**P**		S
Servicios y Soporte								
DS1	Definir niveles de servicio	P	P	**S**	**S**	**S**	S	S
DS2	Administrar Servicios de Terceros	P	P	**S**	**S**	**S**	S	S
DS3	Administrar Desempeño y Capacidad	P	P			**S**		
DS4	Asegurar Servicio Continuo	P	S			**P**		
DS5	Garantizar la Seguridad de Sistemas			**P**	**P**	**S**	S	S
DS9	Administrar la Configuración	P				**S**		S
DS10	Administrar Problemas e Incidentes	P	P			**S**		
DS11	Administrar Datos				**P**			P
DS12	Administrar Instalaciones				**P**	**P**		
DS13	Administrar Operaciones	P	P		**S**	**S**		
Monitoreo								
M1	Monitorear los procesos	P	S	**S**	**S**	**S**	S	S
M2	Evaluar lo adecuado del control Interno	P	P	**S**	**S**	**S**	S	S
M3	Obtener aseguramiento independiente	P	P	**S**	**S**	**S**	S	S
M4	Proveer auditoría independiente	P	P	**S**	**S**	**S**	S	S

Tabla IV.3 Procesos de TI con mayor impacto sobre los Criterios de Información

Dominio	Proceso	Criterios de información: Confidencialidad	Integridad	Disponibilidad
Planeación y Organización				
PO9	Evaluar Riesgos	**P**	**P**	**P**
Adquisición e Implementación				
AI6	Administrar Cambios		**P**	**P**
Servicios y Soporte				
DS5	Garantizar la Seguridad de Sistemas	**P**	**P**	**S**
DS12	Administrar Instalaciones		**P**	**P**

La Tabla IV.4 Descripción de los Procesos de TI, describe los procesos de TI seleccionados basados en el estándar COBIT [1].

IV.1.2.2 Diagnosticar el Nivel de Madurez de los Procesos de TI

Para el diagnostico de los Procesos de TI, se utiliza el CMMI, que permite el análisis y comprensión del ambiente de control de las TI en la empresa.

Las escalas del CMMI ayudan a explicar a los responsables de cada Proceso y a la alta gerencia dónde existen deficiencias en la administración de TI, comparando las prácticas de control de la empresa con los que presenta el estándar COBIT.

Este modelo permite desarrollar un método de puntaje de modo que se pueda calificar a los procesos de TI desde inexistente hasta optimizada (de 0 a 5).

A continuación se lleva a cabo la implementación del CMMI siguiendo la estrategia definida en la Metodología de Gobernabilidad de los Recursos de TI.

IV.1.2.2.1 Estudiar los Procesos de TI

Esta etapa comienza con el análisis de las características de cada nivel de madurez para los proceso de TI seleccionados para la empresa.

Para esta actividad se tienen en cuenta la descripción propuesta por el estándar COBIT para cada nivel del modelo CMMI (Anexo A: Modelo de Madurez). A partir de esta información, se realiza un análisis y adaptación de las condiciones requeridas por los procesos de TI en la empresa.

En la Tabla IV.5 CMMI para los Procesos de TI, resume las condiciones más importantes que los procesos de TI seleccionados deben cumplir para cada uno de los niveles.

Tabla IV.4 Descripción de los Procesos de TI

Procesos de TI	Descripción
Evaluar Riesgos	La evaluación de riesgos es el conjunto de pasos secuenciales, lógicos y sistemáticos que debe seguir el analista de riesgos para identificar, valorar y manejar los riesgos asociados a los procesos del Área de TI, los cuales ejecutados en forma organizada le permiten encontrar soluciones reales a los riesgos detectados, minimizando las pérdidas o maximizando las oportunidades.
Administrar Cambios	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 controladamente. En la Administración de Cambios, los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previo a la implantación y revisar los resultados de los cambios planeados después de la implantación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción. .
Garantizar la Seguridad de sistemas.	La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad
Administrar Instalaciones	El Proceso Administrar Instalaciones debe proporcionar un ambiente físico conveniente, que proteja los equipos y al personal de TI contra peligros naturales o fallas humanas, esto se hace posible a través de la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para garantizar su adecuado funcionamiento.

Tabla IV.5 CMMI para los Procesos de TI

Proceso	Nivel 0: No existente	Nivel 1: Inicial	Nivel 2: Repetible	Nivel 3: Proceso Definido	Nivel 4: Administrado	Nivel 5: Optimizado
Evaluar Riesgos	▪ La evaluación de riesgos para los procesos y las decisiones de negocio no ocurre. ▪ La administración de riesgos no se ha identificado como algo relevante	▪ Los riesgos de TI se toman en cuenta de manera ad hoc. ▪ Existe un entendimiento emergente de que los riesgos de TI son importantes y necesitan ser considerados. ▪ Se realizan evaluaciones informales para cada proyecto	▪ Existe un enfoque de evaluación de riesgos inmaduro y en evolución y se implanta a discreción de los gerentes de proyecto.	▪ Una política de administración de riesgos para toda la organización define cuándo y cómo realizar las evaluaciones de riesgos. ▪ Proceso Documentado. ▪ Personal capacitado	▪ La evaluación y administración de riesgos son procesos estándar. ▪ La administración de riesgos de TI es una responsabilidad de alto nivel.	▪ La captura, análisis y reporte de los datos de administración de riesgos están altamente automatizados. ▪ La dirección evalúa las estrategias de mitigación de riesgos de manera continua.
Administrar Cambios	▪ No existe un proceso definido de administración de cambio y los cambios se pueden realizar sin control.	▪ Se reconoce que los cambios se deben administrar y controlar. ▪ Hay documentación de cambio pobre o no existente y la documentación de configuración es incompleta y no confiable.	▪ Existe un proceso de administración de cambio informal y la mayoría de los cambios siguen este enfoque; sin embargo, el proceso no está estructurado, es rudimentario y propenso a errores.	▪ Existe un proceso formal definido para la administración del cambio, que incluye la categorización, asignación de prioridades, procedimientos de emergencia y autorización del cambio. ▪ Aún pueden ocurrir errores y los cambios no autorizados ocurren ocasionalmente.	▪ El proceso de administración de cambio se desarrolla bien y es consistente para todos los cambios, y la gerencia confía que hay excepciones mínimas. ▪ Hay un proceso consistente para monitorear la calidad y el desempeño del proceso de administración de cambios.	▪ El proceso de administración de cambios se revisa con regularidad y se actualiza para permanecer en línea con las buenas prácticas.
Administrar instalaciones	▪ No hay conciencia sobre la necesidad de proteger las instalaciones o la inversión en recursos de TI ▪ Los factores ambientales tales como protección contra fuego, polvo, tierra y exceso de calor y humedad no se controlan ni se monitorean.	▪ La organización reconoce la necesidad de contar con un ambiente físico que proteja los recursos y el personal contra peligros naturales y causados por el hombre. ▪ La administración de instalaciones y de equipo depende de las habilidades de individuos clave ▪ El personal se puede mover dentro de las instalaciones sin restricción.	▪ La seguridad física es un proceso informal, realizado por un pequeño grupo de empleados con alto nivel de preocupación por asegurar las instalaciones físicas. ▪ Los procedimientos de mantenimiento de instalaciones no están bien documentados y dependen de las buenas prácticas de unos cuantos individuos. ▪ Las metas de seguridad física no se basan en estándares formales.	▪ Se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de cómputo controlado. ▪ Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado. ▪ Los visitantes se registran y acompañan dependiendo del individuo. ▪ Las instalaciones físicas mantienen un perfil bajo y no son reconocibles de manera fácil.	▪ Se entiende por completo la necesidad de mantener un ambiente de cómputo controlado. ▪ Los requerimientos de seguridad físicos y ambientales están documentados y el acceso se monitorea y controla estrictamente. ▪ Están implementados mecanismos de control estandarizados para la restricción de accesos a instalaciones y para contrarrestar los factores ambientales y de seguridad. ▪ La gerencia monitorea la efectividad de los controles y el cumplimiento de los estándares establecidos.	▪ Hay un plan acordado a largo plazo para las instalaciones requeridas para soportar el ambiente de cómputo de la organización. ▪ Los estándares están definidos para todas las instalaciones, incluyendo la selección del centro de cómputo, construcción, vigilancia, seguridad personal, sistemas eléctricos y mecánicos, protección contra factores ambientales ▪ El acceso es monitoreado continuamente y controlado estrictamente con base en las necesidades del trabajo, los visitantes son acompañados en todo momento. ▪ El ambiente se monitorea y controla por medio de equipo especializado y las salas de equipo funcionan sin operadores humanos.

Tabla IV.5 CMMI para los Procesos de TI (Continuación)

Proceso	Nivel 0: No existente	Nivel 1: Inicial	Nivel 2: Repetible	Nivel 3: Proceso Definido	Nivel 4: Administrado	Nivel 5: Optimizado
Garantizar la Seguridad de Sistemas	▪ La responsabilidad no está asignada para garantizar la seguridad de sistema. ▪ Hay una falta total de procesos reconocibles de administración de seguridad de sistemas.	▪ La organización reconoce la necesidad de seguridad para los recursos de TI. ▪ El criterio de la seguridad de TI depende del individuo. ▪ La seguridad de TI ocasiona acusaciones personales, debido a que las responsabilidades no son claras.	▪ Las responsabilidades sobre la seguridad, están asignadas a un coordinador de seguridad de TI, pero la autoridad gerencial del coordinador es limitada. ▪ La conciencia sobre la necesidad de la seguridad esta fraccionada y limitada. ▪ Las políticas de seguridad se han estado desarrollando, las herramientas y las habilidades son inadecuadas. ▪ Los reportes de la seguridad de TI son incompletos, engañosos o no aplicables.	▪ Existe conciencia sobre la seguridad y ésta es promovida por la gerencia. ▪ Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI. ▪ Las responsabilidades de la seguridad de TI están asignadas y entendidas, pero no continuamente implementadas. ▪ Se realizan pruebas de seguridad adecuadas (por ejemplo, pruebas contra intrusos). ▪ Existe capacitación en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal.	▪ Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. ▪ El contacto con métodos para promover la conciencia de la seguridad es obligatorio. ▪ La identificación, autenticación y autorización de los usuarios está estandarizada. ▪ Las pruebas de seguridad se hacen utilizando procesos estándares y formales que llevan a mejorar los niveles de seguridad. ▪ Los procesos de seguridad de TI están coordinados con la función de seguridad de toda la organización. ▪ Los reportes de seguridad están ligados con los objetivos del negocio. ▪ La capacitación sobre seguridad de TI se planea y se administra de manera que responda a las necesidades del negocio y a los perfiles de riesgo de seguridad.	▪ La seguridad en TI es una responsabilidad conjunta del negocio y de la gerencia de TI y está integrada con los objetivos de seguridad del negocio ▪ Los requerimientos de seguridad de TI están definidos de forma clara, optimizados e incluidos en un plan de seguridad aprobado. ▪ Los incidentes de seguridad son atendidos de forma inmediata con procedimientos formales de respuesta soportados por herramientas automatizadas. ▪ Se llevan a cabo valoraciones de seguridad de forma periódica para evaluar la efectividad de la implementación del plan de seguridad. ▪ La información sobre amenazas y vulnerabilidades se recolecta y analiza de manera sistemática. ▪ Se llevan a cabo pruebas de seguridad, análisis de causa-efecto e identificación pro-activa de riesgos para la mejora continua de procesos.

IV.1.2.2.2 Seleccionar parámetros para evaluar procesos de TI

Para evaluar los procesos de TI, se necesita determinar parámetros, que guiarán en el proceso de recolección de información, facilitando a los evaluadores a realizar una rápida evaluación del proceso de TI.

La selección de los parametros para evaluar los proceso de TI se realiza teniendo como referencia las carácterísticas organizacionales de la empresa de seguro y los objetivos de AI, descriptos en la Fase 1, como así también las condiciones de cada nivel de madurez identificadas y resumidas en la Tabla IV.5 CMMI para los Procesos de TI.

Por consiguiente, a continuación se describen los parámetros seleccionados:

• **Relevancia del Proceso:** Este parametro esta asociado a la importancia de los Directivos de la Empresa sobre el Proceso de TI.

•**Políticas:** La política hace referencia al proceso y actividad orientada a la toma de decisiones de un grupo para la consecución de unos objetivos.

•**Procedimientos:** El procedimiento es el modo de ejecutar determinadas acciones que suelen realizarse de la misma forma, con una serie común de pasos claramente definidos, que permiten realizar un trabajo correctamente.

• **Capacitación del Personal:** Este parametro se refiere a la capacitación que recibe el personal asociado al Proceso de TI.

• **Gestión del Proceso:** Se analiza como se lleva a cabo el Proceso de TI evaluado, es decir, si cumple con las funciones por las cuales fue creado.

Una vez definidos los parámetros, se analiza las caracteristicas de los parámetro seleccionados en cada nivel de madurez, el cual facilitará a los encuestados determinar en que nivel se encuentra cada parámetro y determinar una media para evaluar el proceso de TI.

La Tabla IV.6 CMMI de Parámetros, lista las condiciones de cada parámetro seleccionado según los distintos Niveles de Madurez que puede alcanzar.

Tabla IV.6 CMMI de Parámetros

	Parámetros				
Nivel	**Relevancia del Proceso**	**Políticas**	**Procedimientos**	**Capacitación del Personal**	**Gestión del Proceso**
0	No existe reconocimiento de la necesidad del Proceso de TI.	No existen politicas para el Proceso de TI.	No existen Procedimientos para el Proceso de TI.	No existe capacitación del personal.	No existe la gestión para el Proceso de TI.
1	Surge el reconocimiento de la necesidad del Proceso de TI.	Las Politicas para el Proceso de TI no estan definidas.	Existen enfoques ad hoc hacia los procesos y las prácticas. Los procesos y las prácticas no están definidos.	No existe un plan de entrenamiento formal.Las personas toman la propiedad de los problemas con base en su propia iniciativa de manera reactiva.	La Gestión del Proceso de TI se realiza de manera informal.
2	Existe conciencia de la necesidad de actuar.	Existe un entendimiento informal de las politicas sobre el Proceso de TI.	Surgen procesos similares y comunes pero en su mayoría son intuitivos y parten de la experiencia individual. Algunos aspectos de los procesos son repetibles debido a la experiencia individual, y puede existir alguna documentación y entendimiento informal de los procedimientos.	Se da entrenamiento como respuesta a las necesidades, en lugar de hacerlo con base en un plan acordado. Existe entrenamiento informal sobre la marcha.	La Gestion del Proseso de TI es inmadura pero en evolución.
3	La relevancia del Proceso de TI existe de manera parcial hacia los requerimientos.	Las políticas están definidos y documentados para todas las actividades clave.	Surge el uso de buenas prácticas. Se definen y documentan los requerimientos y habilidades para todas las áreas.	Existe un plan de entrenamiento formal pero todavía se basa en iniciativas individuales.	Existe un Proceso formal definido.
4	Hay entendimiento de los requerimientos completos.	La dirección ha definido y aprobado las políticas. Las Politicas estan documentadas.	El proceso es sólido y completo; se aplican las mejores prácticas internas.	Se aplican técnicas maduras de entrenamiento de acuerdo al plan y se fomenta la transmisión del conocimiento.Se evalúa la efectividad del plan de entrenamiento.	El proceso es eficiente y efectivo. Está documentado.
5	Existe un entendimiento avanzado y a futuro de los requerimientos.	La documentación de procesos ha evolucionado a flujos de trabajo automatizados. Las políticas están estandarizados para permitir una administración y mejoras integrales.	Se adoptan y siguen estándares para el desarrollo y mantenimiento de procesos y procedimientos. Se aplican las mejores prácticas.	La organización fomenta de manera formal la mejora continua de las habilidades, con base en metas personales y organizacionales claramente definidas. El entrenamiento y la educación dan soporte a las mejores prácticas externas y al uso de conceptos y técnicas de vanguardia. Se usan a expertos externos y a líderes de la industria como guía.	Proceso optimizado. El parámetro se encuentra automatizado, monitoreado y formalizado.

IV.1.2.2.3 Evaluar Procesos de TI

Esta actividad tiene como finalidad determinar en que nivel de madurez se encuentran los procesos de TI seleccionados en la actividad anterior.

Como se van a evaluar los Procesos de TI, los individuos mas adecuados para realizar dicha tarea son los responsables de los procesos de TI y el personal vinculado con el mismo. Para cada proceso de TI habrá cinco evaluadores, que son el personal vinculado al proceso junto al responsable del mismo.

Para esta actividad se diseña una Hoja de Evaluación (Anexo B: Modelo de Hoja de Evaluación), que tienen como finalidad comparar la situación real del proceso evaluado, con la descripción del nivel de madurez para cada uno de los 5 parámetros seleccionados de cada Proceso de TI, permitiendo también, visualizar el nivel de madurez a alcanzar y establecer las estrategias y políticas necesarias para lograrlo.

Cada evaluador debe realizar una lectura de las caracteristicas de los parámetro en cada nivel de madurez (Tabla IV.6 CMMI de Parámetros), para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

En la Tabla IV.7 Hoja de Evaluación Adaptada a la Empresa, se muestra el modelo propuesto en la Metodología de Gobernabilidad de Recursos de TI, adaptado a la empresa de seguro, con los parámetros seleccionados en la actividad anterior.

Tabla IV.7 Hoja de Evaluación Adapatada a la Empresa

Proceso: Administrar Cambios																		
Parámetros	**Niveles de Madurez**																	
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Inicial**			**Repetible**			**Definido**			**Definido**			**Optimizado**		
Relevancia del Proceso de TI																		
Políticas																		
Procedimientos																		
Capacitación del Personal																		
Gestión del Proceso																		

Los resultados de las Hojas de evaluaciones se encuentran en el Anexo C: Respuestas a la Hoja de Evaluación, a las cuales se le aplica el Modelo Matemático propuesto en la

Metodología de Gobernabilidad para obtener el Nivel de Madurez del Proceso de TI evaluado para ese evaluador.

A continuación se muestra la Tabla IV.8 Resultados de la Hoja de Evaluación que refleja los Resultados Finales para cada Proceso de TI, indicando finalmente, en qué nivel de madurez se encuentran cada uno.

Tabla IV.8 Resultados de la Hoja de Evaluación

	Procesos de TI			
Evaluador	**Evaluar Riesgos**	**Administrar Cambios**	**Garantizar la Seguridad de Sistemas**	**Administrar Instalaciones**
Evaluador 1	2	2	2	3
Evaluador 2	1	1	1	3
Evaluador 3	1	2	1	2
Evaluador 4	1	1	1	3
Evaluador 5	2	1	2	2
Nivel de Madurez	**1**	**1**	**1**	**3**

IV.1.2.2.4 Análisis de resultados.

Para finalizar el análisis de madurez para cada proceso de TI, se detalla a continuación los puntos donde la alta gerencia y los responsables de TI deberían centrar su atención para avanzar hacia una gestión más sistematizada y efectiva.

Evaluar Riesgos.

El proceso de TI Evaluar Riesgos se encuentra en el **nivel 1 Inicial,** y teniendo como referencia los resultados obtenidos, se listan a continuación características que reflejan esta situación:

- La alta gerencia de la empresa de seguro le da importancia solo a los riesgos más relevantes que afectan a las transacciones diarias.
- Existe un entendimiento emergente de que los riesgos de TI son importantes y necesitan ser considerados.
- La empresa es totalmente dependiente de las personas que actúan por iniciativa propia cuando se presentan riesgos, ya que no existen políticas ni procesos formales.

- No hay responsabilidades definidas cuando se presentan riesgos.
- No hay capacitación del personal sobre este proceso de TI.
- Los responsables del Proceso de TI intentan dar respuestas a los riesgos en forma intuitiva.
- No se logra diferenciar ni clasificar los riesgos puesto que no existe una clasificación formal de los mismos ni acciones a llevar a cabo cuando se presentan.

Administrar los cambios.

El Proceso de TI Administrar los cambios, se encuentra en el **nivel 1 Inicial,** ya que posee las siguientes características:

- La alta gerencia de la empresa de seguro reconoce la importancia de este Proceso de TI.
- Hay conciencia por parte de los responsables de este proceso de TI de la necesidad de crear políticas formales para el control de cambios.
- Las actividades de control son realizadas en forma desorganizada, no se identifican procesos claros ni sistematizados, es rudimentario y propenso a errores.
- Hay documentación de cambio insuficiente o no existe.
- Es posible que ocurran errores junto con interrupciones, provocados por una pobre administración de cambios.
- No hay procedimientos formales para la administración de cambios que establezcan un tratamiento de todas las solicitudes de mantenimiento y actualizaciones, en aplicaciones, procesos, servicios y parámetros de sistema.
- No hay capacitación formal.
- La responsabilidad es delegada al individuo.

Garantizar la seguridad de sistemas.

El proceso Garantizar la seguridad de los sistemas, se encuentra en el **nivel 1 Inicial.** Las características generales son:

- La organización reconoce la necesidad de seguridad para los recursos de TI.
- Los incidentes de seguridad de TI ocasionan respuestas individuales, debido a que las responsabilidades no son claras.

- No existen normas formalmente aprobadas ni definidas que alcancen a todo la empresa en materia de seguridad informática.
- El criterio de la seguridad de TI depende del individuo.
- No existe capacitación para el personal relacionado a este proceso de TI.

Administrar Instalaciones.

El Proceso de TI Administrar Instalaciones se encuentra en el **nivel 3 Proceso definido.** Las características generales son:

- La empresa reconoce la necesidad de contar con un ambiente físico que proteja los recursos y el personal contra peligros naturales y causados por el hombre.
- La gerencia monitorea los controles ambientales de las instalaciones o el movimiento del personal.
- Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado.
- Los visitantes se registran y son acompañados por personal de seguridad de la empresa dependiendo del visitante.
- Las instalaciones físicas mantienen un perfil bajo y no son reconocibles de manera fácil.

Los resultados del CMMI refleja que el proceso de **Administrar Instalaciones** es un **proceso definido**, marcando una diferencia en el nivel de maduración con los procesos **Evaluar Riesgos, Administrar Cambios y Garantizar la Seguridad de Sistemas**, que se encuentran en el **nivel Inicial**. Por lo tanto, se considera necesario auditar estos últimos Procesos de TI, para detectar las debilidades e implementar las mejoras necesarias para que estos Procesos de TI evolucionen a un nivel de maduración superior.

IV.1.3 Fase 3: Auditoría Informática

En esta fase se lleva a cabo la AI a los Procesos de TI, para ayudar a los directivos a identificar en qué casos los controles son suficientes, o para asesorarlos respecto a los procesos que requieren ser mejorados. Se diseña un plan de trabajo que guiará al auditor sobre los pasos a seguir, evaluando controles y emitiendo las recomendaciones necesarias.

IV.1.3.1 Elaboración del Plan de trabajo

El plan de trabajo ayuda en la implementación de las buenas prácticas que hacen falta y define una trayectoria de evaluación que permitirá dar seguimiento y continuidad al proceso de mejora continua.

A continuación en la Tabla IV.9 Plan de trabajo, muestra los pasos a seguir para cada proceso de TI seleccionado, según la propuesta en la Metodología de Gobernabilidad de Recursos de TI.

Tabla IV.9 Plan de Trabajo

<table>
<tr><th colspan="5">Plan de Trabajo</th></tr>
<tr><td colspan="4">Objetivo:</td><td>Duración</td></tr>
<tr><td colspan="4">El Plan de Trabajo, será la guía que permita ordenar y sistematizar información relevante para realizar la AI.</td><td>4 meses.</td></tr>
<tr><td colspan="5">Actividades:
▪ Confección de instrumentos para recolección de datos.
▪ Relevamiento y diagnóstico de necesidades para cada proceso de TI.
▪ Observación y análisis de deficiencias.
▪ Emitir recomendaciones.</td></tr>
<tr><td>Procesos</td><td>Documentos a evaluar</td><td>Controles a evaluar</td><td>Objetivo de TI que satisface</td><td>Objetivo de negocio que satisface</td></tr>
<tr><td>Evaluar Riesgos</td><td>▪ Plan de gestión y adecuación de Riesgos.
▪ Políticas y procedimientos relacionados con la evaluación de riesgo.
▪ Documentos de Evaluación de riesgo.</td><td>▪ Evaluación de riesgos.
▪ Medición de riesgos.
▪ Monitoreo de riesgos.</td><td>• Administrar los riesgos asociados al activo (la información) de la empresa.</td><td>• Proteger y responder por todos los activos de TI.
• Mantener la integridad de la información.</td></tr>
<tr><td>Administración de Cambios</td><td>▪ Políticas y procedimientos relacionados con el control de cambios.
▪ Plan de gestión de cambios.</td><td>▪ Solicitud de Cambios
▪ Registro de Cambios
▪ Revisión de Cambios</td><td>• Cumplimiento de políticas internas con respecto al resguardo de la información.</td><td>• Garantizar que la información crítica y confidencial sea resguardada solo para aquello con acceso permitido.</td></tr>
</table>

Tabla IV.9 Plan de Trabajo (Continuación)

Procesos	Documentos a evaluar	Controles a evaluar	Objetivo de TI que satisface	Objetivo de negocio que satisface
Garantizar la Seguridad de sistemas	▪ Procedimientos de administración de cuentas de usuario ▪ Política de seguridad del usuario o de protección de la información. ▪ Procedimientos de seguimiento, solución y escalamiento de problemas ▪ Reportes de violaciones a la seguridad y procedimientos de revisión administrativa.	▪ Seguridad Física. ▪ Seguridad Lógica. ▪ Manipulación / Gestión de Claves / Perfiles / Permisos.	▪ Mejorar la atención de los clientes, reduciendo los tiempos de espera en la tramitación y otorgamiento de beneficios. ▪ Obtener información confiable y útil para la toma de decisiones en materia de crecimiento y asesoramiento en protección de la vida y su patrimonio.	▪ Reducir defectos y tareas repetidas en las soluciones y en la prestación de servicios. ▪ Garantizar que se pueda confiar en las transacciones de negocio y en los intercambios de información automatizados.

IV.1.3.2 Desarrollo del Plan de Trabajo

Para llevar a cabo la AI en cada proceso de TI, como primera instacia, se definen los instrumentos que permiten la recolección de informacón que luego será analizada.

Uno de los instrumentos mas utilizados fueron las entrevistas informales con cuetionario abierto, que giraron en los siguientes temas:

- Funciones y responsabilidades del Area de TI.
- Participación y conocimientos en proyectos de negocio.
- Planes de contingencias que utilizan los responsables de los Procesos de TI.
- Seguridad física y lógica de los sistemas de información.
- Control de cambios de los sistemas de información.

A partir de las entrevistas informales, se preparó una encuesta con preguntas concisas, orientadas para los responsables de los procesos de TI, con el fin de obtener información específica y objetiva para un mejor análisis.

En la estructuración de las encuestas se han considerado las Directrices de Auditoria del estándar COBIT (Anexo F: Directrices de COBIT), esto permite que el auditor pueda

comparar los procesos específicos de TI con los Objetivos de Control de COBIT recomendados. Si bien las Directrices tienen una estructura genérica y de alto nivel, se tiene en cuenta los controles a evaluar en base a las características de la empresa de seguro. (Anexo D: Controles a Evaluar).

A continuación en las Tablas IV.10, IV.11 y IV.12 se muestran las respuestas de los responsables del proceso de TI auditado, que reflejan como se llevan a cabo los controles.

Tabla IV.10 Encuesta de Controles: Evaluar Riesgos

Proceso: Evaluar Riesgos		
Controles a Evaluar	**Cumplimiento del Control**	**Observación**
Existe un marco referencial para la evaluación sistemática de riesgos.	Si ____ No__X_	No se aplica la evaluación sistemática de riesgo a pesar que internamente en la empresa reconocen su importancia.
El marco de referencia incorpora los riesgos de información relevantes para el logro de los objetivos de la empresa.	Si ____ No__X_	
Existe una base que determine la forma en que deben ser manejados los riesgos en un nivel aceptable.	Si ____ No__X_	
El enfoque de evaluación de riesgos asegura la evaluación actualizada de riesgos a nivel global.	Si ____ No__X_	
El enfoque de evaluación de riesgos asegura la evaluación actualizada de riesgos a nivel específico de sistemas.	Si ____ No__X_	
Existen procedimientos de evaluación de riesgos que determinen los factores externo e internos de los riesgos identificados.	Si ____ No__X_	No existen procedimientos de identificación de riesgos ni enfoque de evaluación de riesgos.
Los procedimientos de evaluación de riesgos toman en consideración los resultados de las auditorías, inspecciones, e incidentes identificados.	Si ____ No__X_	Los riesgos de TI se toman en cuenta de manera ad hoc, es decir, se los considera en el momento en que se presentan.
Existe documentación de evaluación de riesgos con la metodología que se usa para tal fin.	Si ____ No__X_	No hay documentación formal para este Proceso.
Existe documentación de evaluación de riesgo que identifique las exposiciones significativas y los riesgos correspondientes	Si ____ No__X_	
Existe un enfoque cuantitativo y/o cualitativo (o combinado) formal para la identificación y medición de riesgos, amenazas y exposiciones.	Si ____ No__X_	• Los controles que definen la identificación de los riesgos no se aplican en la empresa. • No existe una base de riesgos relevantes capaz de determinar cómo estos deben ser administrados. • No existen indicadores para realizar cálculos y otros métodos de medición.
Se incluyen técnicas de probabilidad, frecuencia y análisis de amenazas en la identificación de riesgos.	Si ____ No__X_	
Se utilizan cálculos y otros métodos en la medición de riesgos, amenazas y exposiciones	Si ____ No__X_	
Existen procedimientos para el monitoreo de cambios en la actividad de procesamiento de sistemas.	Si ____ No__X_	• No existen monitoreos definidos en la empresa. • Los riesgos de los cambios y su evaluación son realizados cuando se presentan.
Los procedimientos de monitoreo de cambio determinan que los riesgos y exposición de los sistemas son ajustados oportunamente	Si ____ No__X_	
Existen procedimientos para el monitoreo y el mejoramiento continuos de la evaluación de riesgos.	Si ____ No__X_	

Tabla IV.10 Encuesta de Controles: Evaluar Riesgos (Continuación)

Controles a Evaluar	Cumplimiento del Control	Observación
Los procedimientos para el mejoramiento de la evaluación de riesgos incluyen procesos para la creación de controles que mitiguen los riesgos.	Si ____ No__X_	
El personal asignado a evaluación de riesgos está adecuadamente calificado.	Si ____ No__X_	No hay personal que desempeñe esta actividad
Existe un Plan de acción contra riesgos.	Si ____ No__X_	No existe plan de acción
El plan de acción contra riesgos es utilizado en la implementación de medidas apropiadas para mitigar los riesgos, amenazas y exposiciones.	Si ____ No__X	

Tabla IV.11 Encuesta de Controles: Administrar cambios

Proceso: Administrar Cambios		
Controles a Evaluar	**Cumplimiento del Control**	**Observación**
Existe y se utiliza una metodología para priorizar los requerimientos de los usuarios para cambios al sistema.	Si ____ No__X_	El requerimiento de cambio es anotado en una planilla para su posterior evaluación.
Se consideran procedimientos de cambios de emergencia en los manuales de operaciones.	Si ____ No__X_	
El control de cambios es un procedimiento formal para los usuarios.	Si ____ No__X_	
El control de cambios es un procedimiento formal para los grupos de desarrollo.	Si ____ No__X_	
La bitácora de control de cambios asegura que todos los cambios mostrados fueron resueltos.	Si ____ No__X_	No controla si los cambios fueron realizados
El usuario está satisfecho con el resultado de los cambios solicitados.	Si ____ No__X_	
En la bitácora de control de cambio se especifica si el cambio trajo modificaciones en los programas y operaciones.	Si ____ No__X_	El Área de TI no lleva a cabo controles de cambios
En la bitácora de control de cambio se registra que los cambios hayan sido llevados a cabo como fueron documentados.	Si ____ No__X_	
El proceso de cambios monitorea la mejora en el conocimiento del usuario con respecto al proceso.	Si ____ No__X_	No existe Monitoreo de los cambios.
El proceso de cambios monitores la efectividad en el tiempo de respuesta y satisfacción del usuario con respecto al proceso.	Si ____ No__X_	

Tabla IV.12 Encuesta de Controles: Garantizar la Seguridad de Sistemas

Proceso: Garantizar la Seguridad de Sistemas		
Controles a Evaluar	**Cumplimiento del Control**	**Observación**
Existe un plan de seguridad estratégico.	Si ____ No__X_	No existe un plan de seguridad.
El plan de seguridad estratégico proporciona una dirección y control centralizado sobre la seguridad de los sistemas de información.	Si ____ No__X_	
El plan de seguridad estratégico proporcione los requerimientos de seguridad del usuario como soporte.	Si ____ No__X_	
Se cuenta con una organización de seguridad centralizada responsable de asegurar el acceso apropiado a los recursos del sistema.	Si _X__ No____	Tarea a cargo del Gerente de Sistema.
Se cuenta con un esquema de clasificación de datos que indique que todos los recursos del sistema cuentan con un propietario responsable de su seguridad y contenido.	Si ____ No__X_	
Se cuenta con perfiles de seguridad de usuario.	Si _X__ No____	El Área de TI cumple con esta directriz.

Tabla IV.12 Encuesta de Controles: Garantizar la Seguridad de Sistemas (Continuación)

Proceso: Garantizar la Seguridad de Sistemas		
Controles a Evaluar	**Cumplimiento del Control**	**Observación**
Se revisan regularmente los perfiles de usuarios con fines de re acreditación.	Si _X__ No____	
La empresa brinda capacitación sobre seguridad de sistemas a sus empleados.	Si ____ No__X_	No existe capacitación continua al personal sobre seguridad de los recursos de TI.
El entrenamiento incluye concientización sobre seguridad de sistemas y responsabilidad de propietario.	Si ____ No__X_	
Se capacita sobre los requerimientos de protección contra virus o ataques maliciosos.	Si ____ No__X_	
Se cuenta con reportes de fallas a la seguridad y procedimientos formales de solución de problemas.	Si _X__ No____	El sistema reporta intentos no autorizados de acceso a los recursos del sistema únicamente, vía mail al Gerente de Sistema. El sistema privilegia el acceso a recursos por ID de usuario.
Se cuenta con reportes de Intentos no autorizados de acceso al sistema.	Si _X__ No____	
Se cuenta con reportes de Intentos no autorizados de acceso a los recursos del sistema.	Si _X__ No____	
Se cuenta con reportes de Intentos no autorizados para consultar o modificar las definiciones y reglas de seguridad.	Si ___ No__X__	
Se cuenta con reportes de privilegios de acceso a recursos por ID de usuario.	Si _X__ No____	
Se cuenta con reportes de modificaciones autorizadas a las definiciones y reglas de seguridad.	Si ___ No__X__	
Se cuenta con reportes de accesos autorizados a los recursos.	Si _X__ No____	
Se cuenta con reportes de cambio de estatus de la seguridad del sistema.	Si ___ No__X__	
Se cuenta con reportes de accesos a las tablas de parámetros de seguridad del sistema operativo.	Si ___ No__X__	
Existen módulos criptográficos y procedimientos de mantenimiento de llaves.	Si ___ No__X_	Solo dan de bajas a usuarios que ya no pertenecen a la empresa o modifican el perfil del usuario cuando cambia de un sector a otro, cambiando de grupo.
Los procedimientos de mantenimiento de llaves son administrados de forma centralizada y si son utilizados para todas las actividades de acceso externo y de transmisión.	Si ____ No__X_	
Existen estándares de administración de llaves criptográfica para la actividad centralizada.	Si ____ No__X_	
Existen estándares de administración de llaves criptográfica para los usuarios.	Si ____ No__X_	
Los controles de cambios al software de seguridad son formales y consistentes con los estándares normales de desarrollo y mantenimiento de sistemas.	Si ____ No__X_	
Los mecanismos de autenticidad proveen el uso individual de datos de autenticación (Ej., passwords nunca son reutilizados).	Si ____ No__X_	No se controlan los mecanismos de Autenticidad. (lo único que hace es poder cambiar la clave). El sistema controla la re-autentificación al usuario otras veces después de la autentificación inicial.
Los mecanismos de autenticidad realizan una autentificación múltiple (Ej., se utilizan dos o más mecanismos de autenticación diferentes).	Si ____ No__X_	
Los mecanismos de autenticación es basada en políticas (Ej., capacidad para especificar procedimientos de autenticación separados para eventos específicos).	Si ____ No__X_	
Los mecanismos de autenticación se realiza por demanda (Ej., habilidad para re-autenticar al usuario otras veces después de la autentificación inicial).	Si ____ No__X_	
El número de sesiones concurrentes correspondientes al mismo usuario están limitadas.	Si _X__ No____	Las sesiones al mismo usuario se encuentran limitadas.
Al ingresar al sistema, aparece un mensaje de advertencia preventivo en relación al uso adecuado del hardware, software o conexión.	Si ____ No__X_	
Al lograrse la sesión exitosamente, se despliega el historial de los intentos exitosos y fallidos de acceso a la cuenta del usuario.	Si ____ No__X_	

Tabla IV.12 Encuesta de Controles: Garantizar la Seguridad de Sistemas (Continuación)

Proceso: Garantizar la Seguridad de Sistemas		
Controles a Evaluar	**Cumplimiento del Control**	**Observación**
La política de password fuerza el cambio inicial de la Clave la primera vez de uso.	Si __X__ No___	Se realiza el cambio inicial la primera vez de uso.
La política de password contempla la longitud adecuada mínima del password.	Si ___ No_X_	
La política de password especifica la frecuencia mínima obligada para el cambio de password.	Si ___ No_X_	
La política de password realiza una verificación del password en la lista de valores no permitidos (Ej., verificación de diccionario).	Si ___ No_X_	
La política de password contempla una protección adecuada para los passwords de emergencia.	Si ___ No_X_	
El procedimiento formal para resolución de problemas de ID de usuario, se lo suspende después de 5 intentos de entrada fallidas.	Si _X__ No____	ID de usuario suspendido después de 3 intentos de entrada fallidos.
El procedimiento formal para resolución de problemas de ID de usuario incluye Fecha del último acceso y el número de intentos fallidos se despliega al usuario autorizado una vez ingresado.	Si _X__ No____	Al Usuario NO, esta información se muestra en un panel de control al Gerente de sistema.
El procedimiento formal para resolución de problemas de ID de usuario contempla el tiempo de autenticación es limitado a 5 minutos, después del cual se concluye la sesión.	Si ___ No__X__	
El procedimiento formal para resolución de problemas de ID de usuario, informa al usuario de la suspensión, pero no la razón de la misma.	Si ___ No__X__	
La políticas relacionadas con cargos sensitivos incluyen que empleados en estos puestos sensitivos que permanezcan alejados de la organización durante un periodo adecuado de tiempo cada año calendario (período de vacaciones; durante éste tiempo su user ID es suspendido; y la persona que reemplaza al empleado es instruida en el sentido que debe notificar a la administración si nota cualquier anormalidad relacionada con la seguridad).	Si _X__ No____	Cuando un empleado de cargo sensitivo se aleja de la empresa en un periodo de tiempo, al reemplazante se le asigna un ID y una nueva clave. Cuando regresa el empleado, se le asigna su ID y se elimina el ID del reemplazante.
Se produce una rotación de personal involucrado en actividades sensitivas, sin previa notificación, se realiza de tiempo en tiempo.	Si _X__ No____	
El hardware y software de seguridad, así como los módulos criptográficos, están protegidos contra la intromisión o divulgación.	Si ____ No__X_	
El acceso a los datos de seguridad así como la administración de la seguridad, datos de transacciones sensitivas, passwords y llaves criptográficas se limita a la base de la "necesidad de conocer"	Si _X__ No____	La seguridad se limita el acceso al sistema por parte del usuario con un ID y un password autorizado.
Se utilizan rutas confiables para transmitir información sensitiva no encriptada.	Si ___ No__X_	
Las medidas de control detectivo y preventivo han sido establecidas por la administración para prevenir y detectar virus de computador.	Si __X_ No____	La empresa cuenta con antivirus coorporativo.
Para reforzar la integridad de los valores electrónicos, la empresa posee de lectores de tarjetas protegido contra la destrucción, publicación o modificación de la información de la tarjeta. • La información de la tarjeta (PIN y demás información) se protege contra la divulgación de intruso	Si ___ No__X__	La empresa no posee tarjeta de identificación como una medida de seguridad.
En la empresa la información de la tarjeta (PIN y demás información) se protege contra la divulgación de intruso	Si ___ No__X__	

Otra técnica utilizada fue la observación objetiva, permitiendo hacer precisiones sobre la investigación, antes y después de hacer la investigación. Esto permitió comprobar comentarios y observaciones de las personas entrevistadas enriqueciendo la información.

III.1.3.3 Análisis de Resultados

Después de hacer las encuestas y entrevistas, y haber recolectado los datos, se hizo un análisis de ellos, logrando identificar aquellos controles donde la empresa debe hacer hincapié para alcanzar la gobernabilidad de los recursos de TI.

A continuación se describe el análisis de los resultados obtenidos:

- **Evaluar riesgos**

No existe un pan de gestión de riesgos que permita identificarlos para tomar una acción para prevenirlos, asumirlos, mitigarlos, evitarlos o resolverlos en caso de un incidente, cuantificando costos y probabilidades de ocurrencia.

Informalmente los riesgos tecnológicos se conocen, pero la falta de un inventario completo y detallado de la TI no permite una evaluación formal de éstos que contemple las fortalezas, las oportunidades, las debilidades y las amenazas.

En la empresa las evaluaciones de riesgos se aplican de manera ad hoc, es decir, que no existen políticas y procedimientos formales para la evaluación del riesgo de los recursos de TI.

La empresa se encuentra expuesta a la ocurrencia de hechos imprevistos que pueden generar perjuicios, sin que estén contempladas las medidas a tomar en cada caso.

Se observó que actualmente en la empresa no existe un equipo específico de administración de riesgos.

- **Administrar los cambios**

No hay procedimientos formales para la administración de cambios que establezcan un tratamiento estandarizado de todas las solicitudes de mantenimiento y actualizaciones, en aplicaciones, procesos, servicios.

Tampoco existe un procedimiento alternativo y formal para atender situaciones de emergencia.

Cuando se realizan cambios o actualizaciones no se genera la documentación pertinente.

Pueden surgir errores inadvertidos a partir de cambios no autorizados y/o no probados a los sistemas de información.

No se cuenta con un procedimiento para la gestión de cambios.

- **Proceso: Garantizar la seguridad de sistemas**

No se lleva una gestión centralizada del manejo de la TI, desde donde poder definir e implementar políticas y procedimientos.

No se han establecido los roles, responsabilidades y estándares de TI.

Tampoco existen procedimientos que permitan auditar las acciones de los administradores, usuarios externos e internos y para casos de emergencia.

No hay una política específica que establezca revisiones regulares de todas las cuentas de usuarios y los privilegios asociados.

La ausencia de una administración centralizada de todos los servidores y las cuentas de usuarios, con sus privilegios, permite que la infraestructura de TI y los datos, se encuentren expuestos a ataques internos y externos, con lo que pone en riesgo su disponibilidad e integridad.

Las limitaciones tecnológicas del sistema de comunicaciones por su baja velocidad, no permite dar un servicio remoto eficiente para la administración de usuarios, datos e Internet.

Se detectaron:

- Usuarios comunes con altos privilegios, lo que habilita la posibilidad de instalar aplicaciones no autorizadas.
- Ausencia de herramientas que permitan la detección de intrusos (usuarios no habilitados que puedan acceder a los datos).
- Usuarios genéricos, que no permiten identificar a las personas que acceden y utilizan servicios de TI
- Transmisión de datos sin encriptación. Esto permite la posibilidad de que un tercero, con conocimiento de la información, pueda alterarla.

Se observó también que el personal del área no comprende las consecuencias de un mal manejo de la seguridad de la información, por lo tanto se asignan funciones específicas a personas que no están capacitadas para desempeñar sus tareas eficazmente.

La empresa de seguro no contempla un plan de capacitación para el personal de seguridad de las TI.

IV.1.3.4 Emitir Recomendaciones

Con el apoyo de las Directrices de COBIT se realiza las recomendaciones de mejoras correspondientes a las debilidades encontradas en la AI, las cuales si son implementadas, podemos decir que los objetivos de TI y los objetivos estratégicos de la empresa de seguro estarían alineados, encauzando a la misma hacia la gobernabilidad para la seguridad de la información.

A continuación se realizan las recomendaciones para cada Proceso de TI auditado:

- **Proceso Evaluar riesgo**

Con las debilidades encontradas para este proceso en la AI, se recomienda que la Alta Gerencia apoye la implantación de las siguientes buenas prácticas:

- Diseñar, establecer y hacer cumplir una política de seguridad escrita que sea adoptada en toda la empresa de seguro y que enumere procedimientos claros para apoyar los objetivos de seguridad de las TI en la misma.
- La alta Gerencia debe acompañar las iniciativas de seguridad de las TI y asegurar que el Gerente de TI entienda las necesidades de seguridad del negocio y los procesos necesarios para cubrir dichas necesidades.
- Se deben identificar todas aquellas amenazas y vulnerabilidades que tengan un impacto potencial sobre las metas o las operaciones de la empresa. Determinar la naturaleza del impacto y dar mantenimiento a esta información.
- Definir las funciones y designar responsabilidades del personal clave de seguridad en el área de TI.
- Impartir capacitación frecuente y obligatoria a todos los empleados relativa a la concienciación en seguridad de TI.
- Contratar un equipo especializado, con conocimientos acreditados de seguridad de las TI, o asegurar que los empleados de seguridad son lo suficientemente expertos para asumir las funciones y responsabilidades asignadas.
- Diseñar una planificación a corto y medio plazo, detallando cómo implementar mejoras en la infraestructura de seguridad.
- La documentación de evaluación de riesgos debe incluir:
    - Una descripción de la metodología de evaluación de riesgos.

  - La identificación de exposiciones significativas y los riesgos correspondientes.
  - Los objetivos de toda la organización deben ser incluidos en el proceso de identificación de riesgos.
  - Se incluyen técnicas de probabilidad, frecuencia y análisis de amenazas en la identificación de riesgos.
- La empresa de seguro deberá diseñar un marco referencial para la evaluación sistemática de riesgos, incorporando los riesgos de información relevantes para el logro de los objetivos de la empresa y formando una base para determinar la forma en que los riesgos deben ser manejados a un nivel aceptable.
- Deben existir procedimientos para el monitoreo y el mejoramiento continuos de la evaluación de riesgos y procesos para la creación de controles que mitiguen los riesgos.

- **Proceso Administración de cambios**

"El objetivo de la administración de cambios es proporcionar un proceso disciplinado para incorporar los cambios necesarios al entorno de TI con la interrupción mínima de las operaciones en curso." <15>

Para alcanzar esta meta, teniendo en cuenta las directrices de Auditoria del estándar COBIT, el proceso de administración de cambios debe:

- Tener una metodología de trabajo en el área de TI para priorizar los requerimientos de cambios a los sistemas de información por parte de los usuarios de la empresa de seguro.
- El pedido de cambio se debe realizar de manera formal al área de TI mediante el envío de una solicitud de cambio.
- Se debe asignar una prioridad y una categoría al cambio tras valorar su urgencia e impacto. Se involucra a los responsables de los procesos que podrían verse afectados.
- Tratar el pedido de cambio con la Alta Gerencia de la empresa de seguro para que se apruebe o rechace el cambio.
- Planear la implementación del cambio.
- El Gerente del área de TI debe colaborar con el lanzamiento y la implementación de los cambios aprobados.

- Monitorear la implementación para determinar si el cambio ha alcanzado sus objetivos y si se mantiene o deshace el cambio.
- Realizar un inventario de cambios.
- El proceso de cambios tiene que ser monitoreado en cuanto a mejoras en el conocimiento, efectividad en el tiempo de respuesta y satisfacción del usuario con respecto al proceso.

- **Proceso Garantizar la seguridad de sistemas.**

Las recomendaciones para este proceso son:

- La empresa de seguro debe contar con un plan de seguridad estratégico que proporcione una dirección y control centralizados sobre la seguridad de los sistemas de información, así como requerimientos de seguridad de usuario, como soporte, el cual debe ser acordado entre la Alta Gerencia y el Gerente de TI.
- La capacitación del personal debe incluir un conocimiento y conciencia sobre seguridad, las responsabilidades de los propietarios y los requerimientos de protección contra virus.
- El reporte de fallas a la seguridad y procedimientos formales de solución de problemas deben incluir:
    - Intentos no autorizados de acceso al sistema.
    - Intentos no autorizados de acceso a los recursos del sistema.
    - Intentos no autorizados para consultar o modificar las definiciones y reglas de seguridad.
    - Privilegios de acceso a recursos por ID de usuario.
    - Modificaciones autorizadas a las definiciones y reglas de seguridad.
    - Accesos autorizados a los recursos (seleccionados por usuario o recurso).
    - Cambio de estatus de la seguridad del sistema.
- El número de sesiones concurrentes correspondientes al mismo usuario deben estar limitadas.
- La política de password debe incluir:
    - Forzar el cambio inicial de password la primera vez de uso.

- Longitud adecuada mínima del password.
- La frecuencia obligada mínima de cambio de password.
- Verificación del password en la lista de valores no permitidos (Ej., verificación de diccionario).
- Protección adecuada para los passwords de emergencia.

- Las medidas de control detectivo y preventivo han sido establecidas por la administración para prevenir y detectar virus de computador.

IV.1.4 Etapa de Seguimiento

La etapa de seguimiento y control de las recomendaciones propuestas en la AI queda fuera del alcance de esta tesis.

Se recomienda, para llevar a cabo esta etapa, nombrar un equipo de implementación formado por directivos, gerentes de áreas y coordinados por el responsable interno nombrado en las primeras etapas. Esta etapa de Seguimiento es tarea del equipo de implementación.

La empresa debe seguir las recomendaciones realizadas en la Metodología de Gobernabilidad de Recursos de TI propuesta por los responsables del trabajo de cómo llevarla a cabo.

En un periodo de seis meses, se realiza un estudio de los resultados de seguimiento donde son analizadas las desviaciones ocurridas respecto a lo planificado, para hacer las correcciones necesarias.

Se recomienda que luego de dos años, se realice una nueva autoevaluación de la madurez de los Procesos de TI, volviendo a la Fase 1 de la Metodología de Gobernabilidad, entendiendo que el proceso de maduración del Gobierno de las TI es un proceso de mejora continua.

Este trabajo final utilizó a la AI como herramienta para encauzar la Gobernabilidad de los Recursos de TI, puesto que identificó las debilidades en Procesos de TI seleccionados, y luego se realizó las recomendaciones necesarias, basándose en el estándar COBIT, para que los recursos de TI den respuestas a los objetivos de negocio de la empresa.

Un reto importante que se encontró en el comienzo en este trabajo de tesis, fue, no contar con una Metodología de GTI clara y definida, que integre a la AI como herramienta para encaminar a una empresa hacia la Gobernabilidad de los Recursos de TI. Es por ello, la propuesta de una metodología representó una oportunidad para alcanzar los objetivos de este trabajo final.

En este contexto, las pequeñas y medianas empresas, de nuestro medio, generalmente se enfrentan ante problemas por su bajo nivel de control y por el uso ineficiente de recursos de TI, lo cual es causado por la baja concientización sobre GTI, que desencadenan en una insuficiente definición y una carencia de evaluación de procesos de TI y en la falta de iniciativa para la mejora continua. El mito de pensar que COBIT es un estandar solo para grandes empresas o que es solo para auditores, es generado por el desconocimiento de COBIT y los beneficios que traería su uso en pequeñas o medianas empresas que están en un continuo crecimiento. Ante esta situación, la Metodología de Gobernabilidad, aplicada en una empresa de seguro de nuestro medio, propone una guía para encauzar la Gobernabilidad, utilizando a la AI como herramienta, basada en el estándar COBIT. Las herramientas Tecnológicas incorporadas en la Metodología de Gobernabilidad (CMMI y COBIT), que generalmente son aplicadas en grande organizaciones, han sido adaptadas a esta pequeña empresa proponiendo soluciones concretas a partir de la evaluación y mejora de procesos de TI, ayudando a monitorear y evaluar actividades de TI, de manera que se puedan controlar y tomar decisiones eficientes.

El desconocimiento del concepto de Gobernabilidad y del estándar COBIT, de todo el personal de la empresa bajo estudio, fue un factor en contra, que hizo que el personal sea renuente a participar y brindar la información requerida. Sin embargo, durante la aplicación de la metodología, la alta dirección se dio cuenta del impacto significativo que la información tiene para el éxito de la empresa y de la posibilidad de que sea aprovechada al máximo para tener una ventaja competitiva. Esta visión de la alta gerencia, a cerca de la

importancia de la información para su empresa se trasladó en un apoyo muy importante a la hora de dar confianza a su personal para que participe en este trabajo.

Los responsables de los procesos de TI encuestados hicieron recomendaciones sobre el nivel de tecnicismo en el lenguaje utilizado en los cuestionarios destinados a la evaluación de controles; es por ello que esta herramienta de evaluación fue adaptada a la terminología acorde a las recomendaciones recibidas.

Otro reto importante fue como implementar el CMMI en el presente trabajo, ya que este modelo nos dice el **qué** y no el **cómo**. En el momento implementarlo, no se encontraba una metodología ni un modelo matemático que se adecúe a las necesidades de nuestro objetivo. Estas cuestiones han llevado a establecer el modelo matemático propuesto, determinando el estado de madurez de los procesos de TI seleccionados, para luego ser auditados.

La Metodología de Gobernabilidad de Recursos de TI fue creada de acuerdo a un objetivo que cumple satisfactoriamente: conduce correctamente en la ejecución de sus fases, actividades y tareas, utilizando a la AI como herramienta, emitiendo recomendaciones, que si son llevadas a cabo, encauza a la gobernabilidad de la empresa. Realizamos esta afirmación, ya que se cumplen todos los objetivos específicos propuestos en este trabajo.

Como la metodología tiene como herramienta principal a la AI, la cual está basada en el estándar COBIT, el cual es un marco de referencia para el GTI, desde la dentición de los procesos de TI hasta las recomendaciones realizadas a los procesos de TI auditados, creemos que encauza a la empresa a la Gobernabilidad de los recursos de TI.

Cuando decimos que la Metodología de Gobernabilidad de Recursos de TI encauza la Gobernabilidad, hacemos referencia a que dirige, educa, encamina, guía, y prepara a la empresa al alineamiento de las TI con la estrategia del negocio.

Como la implementación de las recomendaciones no se encuentra en el alcance de la tesis, será el equipo de implementación de la empresa el que llevará a cabo esta etapa, elaborando un plan de acción que se ajuste a las características propias de la empresa.

Por grandes que sean los esfuerzos y aportes de la AI, no habrá valor agregado en tanto la alta gerencia no asuma este papel y se comprometa con la implementación de las recomendaciones propuestas.

En un futuro la empresa de seguro debería implementar la Metodología de Gobernabilidad de Recursos de TI estableciendo como prioridad los requerimientos de negocios para la

información no contemplados en el presente trabajo, tales como requerimientos de calidad y fiduciarios de la información.

Considerando la experiencia obtenida a lo largo del desarrollo del trabajo final surgen algunos puntos a considerar en futuras investigaciones:

- Esta investigación abrirá nuevos caminos para empresas que presenten situaciones similares a la que aquí se plantea, sirviendo como marco referencial a estas.
- Mejorar la Propuesta Metodológica, por ejemplo, en la selección de los procesos de TI, teniendo en cuenta las nuevas versiones del estándar COBIT.
- Automatizar la Metodología de Gobernabilidad de Recursos de TI para facilitar la implementación de la misma.

Bibliografía

[1] IT Governance Institute (ITGI, por sus siglas en Inglés), Comité Directivo de COBIT 4.0 y El IT Governance Institute MR, COBIT® 4.0.

[2] Mario G. Piattini – Emilio del Peso, Ma. 2007, AUDITORÍA INFORMÁTICA Un enfoque Práctico. Editorial Alfaomega Ra –.

[3] IT Governance Institute MR, Herramientas de Implementación, COBIT® 3.

[4] IT Governance Institute MR, Marco de Referencia, COBIT® 3.

[5] Belden Menkus, Auditoría Informática, Objetivos de Control, Controles en un entorno informatizado: Objetivos, Directivas y procedimientos de Auditoría. CISA, CSP Editor.

[6] Lic. Horacio Kuna, Asistente para la realización de auditoría de sistemas en organismos públicos o privados.

[7] López Solís, Rosa Idolina, Diciembre 2003, Modelo para medir la madurez de los procesos y funciones del HelpDesk, Tesis de Maestría en Ciencias en Tecnología Informática del ITESM, Monterrey, N.L., México,. Disponible en: http://biblioteca. itesm.mx.

[8] Concha Huarato, Nancy Elizabet, Propuesta para Implementar CMMI en una empresa para Múltiples Unidades Desarrolladores de Software.

[9] Mario G. Piattini, Emilio del Peso, Julio 2007, Auditoría Informática Un enfoque práctico, 2ª edición. Ampliada y revisada.; Alfaomega Grupo Editor.

[10] López Solís, Rosa Idolina, Diciembre 2003, Modelo para medir la madurez de los procesos y funciones del HelpDesk, Tesis de Maestría en Ciencias en Tecnología Informática del ITESM, Monterrey, N.L, México. Disponible en: http://biblioteca. itesm.mx

[11] Enrique Hernández Hernández Auditoría Informática: un enfoque metodológico; CECSA, México, 2000.

[12] Lic. Fabián Chiara, Noviembre 2007, Congreso: Seguridad de la Información – Integración de Metodologías para su Gestión.. UCSE..

[13] Huidobro Moya – David Roldán Martinez, Seguridad en Redes y Sistemas de Información. José M. Editorial Thomson – Paraninfo.

[14] Kenneth C. Laudon, 2008, Sistemas de Información Gerencial: Administración de la Empresa Digital –– Jane P. Laudon. Editorial PEARSON EDUCACIÓN. México.

Referencias WEB:

<1> Instituto de Gobierno de Tecnología de la Información, Disponible en: http://www.itgi.org/

<2> Agaex Informática: empresa de desarrollo de Software, Disponible en: http://www.agaex.com:8080/ ploneagaex /productos.

<3> COBIT y su implementación en la banca de América Latina, http://www.borrmart.es/ articulo_redseguridad.php?id=1246&numero=25.

<4> Implementación de COBIT en Empresas Internacionales http: //www.pressroom.ups. com /mediakits/factsheet.html

<5> El caso de éxito de la empresa CTFS fue obtenido de ISACA, Disponible: en http://www.isaca.org/

<6> ISACA (Information Systems Audit and Control Association) https://www.isaca.org/Pages/default.aspx

<7> Definición de Gobierno de TI http://www.tgti.es/?q=node/57

<8>Implantación de Gobierno de TI http://www.network-sec.com/contenidos/Gobierno_TI .pdf

<9> Generalidades en la Auditoría http://www.eumed.net/cursecon/libreria/rgl-genaud /1x.htm

<10> Wikipedia. Información. Consultado: Septiembre 2008. Disponible en: http://es.wikipedia.org /wiki/Informacion.

<11> Estrategia, startups y modelos de negocio diferentes. http://javiermegias.com/blog /2009/06/gobierno-de-las-ti/

<12> Metodologías de Auditoria Informática http://es.scribd.com/doc/66204363/19/ METODOLOGIAS-DE-AUDITORIA-INFORMATICA#outer_page_5

<13> IEEE Technology Management Council España – Metodologias y Normas Para Gobierno de TI http://sites.ieee.org/spain-tmc/2011/07/30/metodologias-y-normas-para-gobierno-de-ti-2/

<14>Evaluación del Nivel de Madurez - CMMI – Wikipedia Disponible en : http://es.wikipedia.org/wiki/Capability_Maturity_Model_Integration

ANEXO A

DESCRIPCIÓN DEL MODELO DE MADUREZ POR PROCESO

Descripción del Modelo de Madurez por Proceso [1]

- **Proceso Evaluar Riesgo.**

0 No Existente: es cuando la evaluación de riesgos para los procesos y las decisiones de negocio no ocurre. La organización no toma en cuenta los impactos en el negocio asociados a las vulnerabilidades de seguridad y a las incertidumbres del desarrollo de proyectos. La administración de riesgos no se ha identificado como algo relevante para adquirir soluciones de TI y para prestar servicios de TI.

1 Inicial/Ad Hoc: es cuando los riesgos de TI se toman en cuenta de manera ad hoc. Se realizan evaluaciones informales de riesgos según lo determine cada proyecto. En algunas ocasiones se identifican evaluaciones de riesgos en un plan de proyectos pero se asignan a gerentes específicos con poca experiencia. Los riesgos específicos relacionados con TI tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto. Los riesgos relativos a TI que afectan las operaciones del día con día, son rara vez discutidas en reuniones gerenciales. Cuando se toman en cuenta los riesgos, la mitigación es inconsistente. Existe un entendimiento emergente de que los riesgos de TI son importantes y necesitan ser considerados.

2 Repetible: es cuando existe un enfoque de evaluación de riesgos inmaduro y en evolución y se implanta a discreción de los gerentes de proyecto. La administración de riesgos se da por lo general a altos niveles y se aplica de manera típica solo a proyectos grandes o como respuesta a problemas. Los procesos de mitigación de riesgos están en implantación donde se identifican riesgos.

3 Definido: es cuando existe una política de administración de riesgos para toda la organización, define cuándo y cómo realizar las evaluaciones de riesgos. La administración de riesgos sigue un proceso definido el cual está documentado. El entrenamiento sobre administración de riesgos está disponible para todo el personal. La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento se delega a la discreción del individuo. La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgos claves sean identificados. Un proceso para mitigar los riesgos clave por lo general se institucionaliza una vez que los riesgos se identifican. Las descripciones de puestos toman en cuenta las responsabilidades de administración de riesgos.

4 Administrado: es cuando la evaluación y administración de riesgos son procesos estándar. Las excepciones al proceso de administración de riesgos se reportan a la gerencia de TI. La administración de riesgos de TI es una responsabilidad de alto nivel. Los riesgos se evalúan y se mitigan a nivel de proyecto individual y también por lo regular se hace con respecto a la operación global de TI. La gerencia recibe notificación sobre los cambios en el ambiente de negocios y de TI que pudieran afectar de manera significativa los escenarios de riesgo relacionados con la TI. La gerencia puede monitorear la posición de riesgo y tomar decisiones informadas respecto a la exposición que está dispuesta a aceptar. Todos los riesgos identificados tienen un propietario denominado, y la alta dirección, así como la gerencia de TI han determinado los niveles de riesgo que la organización está dispuesta a tolerar. La gerencia de TI ha elaborado medidas estándar para evaluar el riesgo y para definir las proporciones riesgo/retorno. La gerencia presupuesta para que un proyecto operativo de administración de riesgos re-evalúe los riesgos de manera regular. Se establece una base de datos administrativa y parte del proceso de administración de riesgos se empieza a automatizar. La gerencia de TI toma en cuenta las estrategias de mitigación de riesgo.

5 Optimizado: es cuando la administración de riesgos ha evolucionado al nivel en que un proceso estructurado está implantado en toda la organización y es bien administrado. Las buenas prácticas se aplican en toda la organización. La captura, análisis y reporte de los datos de administración de riesgos están altamente automatizados. La orientación se toma de los líderes en el campo y la organización de TI participa en grupos de interés para intercambiar experiencias. La administración de riesgos está altamente integrada en todo el negocio y en las operaciones de TI está bien aceptada, y abarca a los usuarios de servicios de TI. La dirección detectará y actuará cuando se realicen decisiones grandes de inversión, operación o de TI, sin tomar en cuenta el plan de administración de riesgos. La dirección evalúa las estrategias de mitigación de riesgos de manera continua.

- **Administrar Cambios**

0 No Existente: es cuando 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 TI y las operaciones del negocio, y no hay conciencia de los beneficios de la buena administración de cambio.

1 Inicial/Ad Hoc: es cuando 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.

2 Repetible: es cuando existe un proceso de administración de cambio informal y la mayoría de los 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.

3 Definido: es cuando existe un proceso formal definido para la administración del cambio, que incluye la categorización, asignación de prioridades, procedimientos de emergencia, autorización del cambio y administración de liberación, y va surgiendo el cumplimiento. Se dan soluciones temporales a los problemas y los procesos a menudo se omiten o se hacen a un lado. Aún pueden ocurrir errores y los cambios no autorizados ocurren ocasionalmente. El análisis de impacto de los cambios de TI en operaciones de negocio se está volviendo formal, para apoyar la implantación planeada de nuevas aplicaciones y tecnologías.

4 Administrado: es cuando el proceso de administración de cambio se desarrolla bien y es consistente para todos los cambios, y la gerencia confía que hay excepciones mínimas. El proceso es eficiente y efectivo, pero se basa en manuales de procedimientos y controles considerables para garantizar el logro de la calidad. Todos los cambios están sujetos a una planeación minuciosa y a la evaluación del impacto para minimizar la probabilidad de tener problemas de post-producción. Se da un proceso de aprobación para cambios. La documentación de administración de cambios es vigente y correcta, con seguimiento formal a los cambios. La documentación de configuración es generalmente exacta. La planeación e implantación de la administración de cambios en TI se van integrando con los cambios en los procesos de negocio, para asegurar que se resuelven los asuntos referentes al entrenamiento, cambio organizacional y continuidad del negocio. Existe una coordinación creciente entre la administración de cambio de TI y el rediseño del proceso de negocio. Hay un proceso consistente para monitorear la calidad y el desempeño del proceso de administración de cambios.

5 Optimizado: es cuando el proceso de administración de cambios se revisa con regularidad y se actualiza para permanecer en línea con las buenas prácticas. El proceso de revisión refleja los resultados del monitoreo. La información de la configuración es computarizada y proporciona un control de versión. El rastreo del cambio es sofisticado e incluye herramientas para detectar software no autorizado y sin licencia. La administración de cambio de TI se integra con la administración de cambio del negocio para garantizar que TI sea un factor que hace posible el incremento de productividad y la creación de nuevas oportunidades de negocio para la organización.

- **Administrar Instalaciones**

0 No-existente: es cuando no hay conciencia sobre la necesidad de proteger las instalaciones o la inversión en recursos de cómputo. Los factores ambientales tales como protección contra fuego, polvo, tierra y exceso de calor y humedad no se controlan ni se monitorean.

1 Inicial/Ad Hoc: es cuando la organización reconoce la necesidad de contar con un ambiente físico que proteja los recursos y el personal contra peligros naturales y causados por el hombre. La administración de instalaciones y de equipo depende de las habilidades de individuos clave. El personal se puede mover dentro de las instalaciones sin restricción. La gerencia no monitorea los controles ambientales de las instalaciones o el movimiento del personal.

2 Repetible: es cuando los controles ambientales se implementan y monitorean por parte del personal de operaciones. La seguridad física es un proceso informal, realizado por un pequeño grupo de empleados con alto nivel de preocupación por asegurar las instalaciones físicas. Los procedimientos de mantenimiento de instalaciones no están bien documentados y dependen de las buenas prácticas de unos cuantos individuos. Las metas de seguridad física no se basan en estándares formales y la gerencia no se asegura de que se cumplan los objetivos de seguridad.

3 Definido: es cuando se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de cómputo controlado. Los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con presupuesto autorizado y rastreado por la gerencia. Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado. Los visitantes se registran y acompañan dependiendo del individuo. Las instalaciones físicas mantienen un perfil bajo y

no son reconocibles de manera fácil. Las autoridades civiles monitorean al cumplimiento con los reglamentos de salud y seguridad. Los riesgos se aseguran con el mínimo esfuerzo para optimizar los costos del seguro.

4 Administrado: es cuando se entiende por completo la necesidad de mantener un ambiente de cómputo controlado y se evidencia en la estructura organizacional y en la distribución del presupuesto. Los requerimientos de seguridad físicos y ambientales están documentados y el acceso se monitorea y controla estrictamente. Se establecen y comunican las responsabilidades. El personal de las instalaciones ha sido entrenado por completo respecto a situaciones de emergencia, así como en prácticas de salud y seguridad. Están implementados mecanismos de control estandarizados para la restricción de accesos a instalaciones y para contrarrestar los factores ambientales y de seguridad. La gerencia monitorea la efectividad de los controles y el cumplimiento de los estándares establecidos. La capacidad de recuperación de los recursos de cómputo se incorpora en un proceso organizacional de administración de riesgos. La información integrada se usa para optimizar la cobertura de los seguros y de los costos asociados.

5 Optimizado: es cuando hay un plan acordado a largo plazo para las instalaciones requeridas para soportar el ambiente cómputo de la organización. Los estándares están definidos para todas las instalaciones, incluyendo la selección del centro de cómputo, construcción, vigilancia, seguridad personal, sistemas eléctricos y mecánicos, protección contra factores ambientales (por ejemplo, fuego, rayos, inundaciones, etc.). Se clasifican y se hacen inventarios de todas las instalaciones de acuerdo con el proceso continuo de administración de riesgos de la organización. El acceso es monitoreado continuamente y controlado estrictamente con base en las necesidades del trabajo, los visitantes son acompañados en todo momento. El ambiente se monitorea y controla por medio de equipo especializado y las salas de equipo funcionan sin operadores humanos. Los programas de mantenimiento preventivo fomentan un estricto apego a los horarios y se aplican pruebas regulares a los equipos sensibles. Las estrategias de instalaciones y de estándares están alineadas con las metas de disponibilidad de los servicios de TI y están integradas con la administración de crisis y con la planeación de continuidad del negocio.

- **Garantizar la Seguridad de los Sistemas**

0 No Existente: es cuando la organización no reconoce la necesidad de la seguridad para TI. Las responsabilidades y la rendición de cuentas no están asignadas para garantizar la seguridad. Las medidas para soportar la administrar la seguridad de TI no están implementadas. No hay reportes de seguridad de TI ni un proceso de respuesta para resolver brechas de seguridad de TI. Hay una total falta de procesos reconocibles de administración de seguridad de sistemas.

1 Inicial/Ad Hoc: es cuando la organización reconoce la necesidad de seguridad para TI. La conciencia de la necesidad de seguridad depende principalmente del individuo. La seguridad de TI se lleva a cabo de forma reactiva. No se mide la seguridad de TI. Las brechas de seguridad de TI ocasionan respuestas con acusaciones personales, debido a que las responsabilidades no son claras. Las respuestas a las brechas de seguridad de TI son impredecibles.

2 Repetible pero intuitivo cuando las responsabilidades y la rendición de cuentas sobre la seguridad, están asignadas a un coordinador de seguridad de TI, pero la autoridad gerencial del coordinador es limitada. La conciencia sobre la necesidad de la seguridad esta fraccionada y limitada. Aunque los sistemas producen información relevante respecto a la seguridad, ésta no se analiza. Los servicios de terceros pueden no cumplir con los requerimientos específicos de seguridad de la empresa. Las políticas de seguridad se han estado desarrollando, pero las herramientas y las habilidades son inadecuadas. Los informes de la seguridad de TI son incompletos, engañosos o no aplicables. La capacitación sobre seguridad está disponible pero depende principalmente de la iniciativa del individuo. La seguridad de TI es vista primordialmente como responsabilidad y disciplina de TI, y el negocio no ve la seguridad de TI como parte de su propia disciplina.

3 Definido: es cuando existe conciencia sobre la seguridad y ésta es promovida por la gerencia. Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI. Las responsabilidades de la seguridad de TI están asignadas y entendidas, pero no continuamente implementadas. Existe un plan de seguridad de TI y existen soluciones de seguridad motivadas por un análisis de riesgo. Los informes no contienen un enfoque claro de negocio. Se realizan pruebas de seguridad adecuadas (por ejemplo, pruebas contra intrusos). Existe capacitación en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal.

4 Administrado: es cuando las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. Regularmente se lleva a cabo un análisis de impacto y de riesgos de seguridad. Las políticas y prácticas de seguridad se complementan con referencias de seguridad específicas. El contacto con métodos para promover la conciencia de la seguridad es obligatorio. La identificación, autenticación y autorización de los usuarios está estandarizada. La certificación en seguridad es buscada por parte del personal que es responsable de la auditoría y la administración de la seguridad. Las pruebas de seguridad se hacen utilizando procesos estándares y formales que llevan a mejorar los niveles de seguridad. Los procesos de seguridad de TI están coordinados con la función de seguridad de toda la organización. Los informes de seguridad están ligados con los objetivos del negocio. La capacitación sobre seguridad se imparte tanto para TI como para el negocio. La capacitación sobre seguridad de TI se planea y se administra de manera que responda a las necesidades del negocio y a los perfiles de riesgo de seguridad.

5 Optimizado cuando la seguridad en TI es una responsabilidad conjunta del negocio y de la gerencia de TI y está integrada con los objetivos de seguridad del negocio en la corporación. Los requerimientos de seguridad de TI están definidos de forma clara, optimizados e incluidos en un plan de seguridad aprobado. Los usuarios y los clientes se responsabilizan cada vez más de definir requerimientos de seguridad, y las funciones de seguridad están integradas con las aplicaciones en la fase de diseño. Los incidentes de seguridad son atendidos de forma inmediata con procedimientos formales de respuesta soportados por herramientas automatizadas. Se llevan a cabo valoraciones de seguridad de forma periódica para evaluar la efectividad de la implementación del plan de seguridad. La información sobre amenazas y vulnerabilidades se recolecta y analiza de manera sistemática. Se recolectan e implementan de forma oportuna controles adecuados para mitigar riesgos. Se llevan a cabo pruebas de seguridad, análisis de causa-efecto e identificación pro-activa de riesgos para la mejora continua de procesos. Los procesos de seguridad y la tecnología están integrados a lo largo de toda la organización.

ANEXO B

MODELO DE HOJA DE EVALUACIÓN

Proceso: Evaluar Riesgos

Descripción del Proceso: La evaluación de riesgos es el conjunto de pasos secuenciales, lógicos y sistemáticos para identificar, valorar y manejar los riesgos asociados a los procesos del Área de TI, los cuales ejecutados en forma organizada le permiten encontrar soluciones reales a los riesgos detectados.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Evaluar Riesgos																		
Parámetros	**Niveles de Madurez**																	
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI																		
Políticas																		
Procedimientos																		
Capacitación del Personal																		
Gestión del Proceso																		

Número de Casillas Puntuadas																		
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5		
Puntos obtenidos por cada columna (n° de casillas x valor)																		
Resultado Final																		

Gracias por responder la Hoja de Evaluación

Proceso: Administrar Cambios

Descripción del Proceso: La administración de cambio es el conjunto de acciones que se deben llevar a cabo formalmente y controladamente para todos los cambios, sean estos de infraestructura o aplicaciones. Los cambios de procedimientos, procesos, sistema deben ser registrados, evaluados y autorizados para su implementación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Administrar cambios																		
Parámetros	**Niveles de Madurez**																	
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI																		
Políticas																		
Procedimientos																		
Capacitación del Personal																		
Gestión del Proceso																		

Número de Casillas Puntuadas																		
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5		
Puntos obtenidos por cada columna (n° de casillas x valor)																		
Resultado Final																		

Gracias por responder la Hoja de Evaluación

Proceso: Administrar Instalaciones

Descripción del Proceso: El proceso Administrar Instalaciones requiere de instalaciones bien diseñadas y bien administradas, para obtener la protección de los equipos y del personal. El proceso de Administrar Instalaciones incluye la definición de los requerimientos físicos del área de sistemas, la selección de instalaciones apropiadas y el diseño de procesos efectivos para administrar el acceso físico.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Administrar Instalaciones																		
Parámetros	**Niveles de Madurez**																	
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI																		
Políticas																		
Procedimientos																		
Capacitación del Personal																		
Gestión del Proceso																		

Número de Casillas Puntuadas																		
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5		
Puntos obtenidos por cada columna (n° de casillas x valor)																		
Resultado Final																		

Gracias por responder la Hoja de Evaluación

Proceso: Garantizar la Seguridad de Sistemas

Descripción del Proceso: Garantizar la Seguridad de los Sistemas requiere de un proceso de Administración de Seguridad que permita mantener la integridad de la información y de proteger los activos de TI. Este proceso incluye establecer roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreo de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Garantizar la Seguridad de Sistemas																		
Parámetros	**Niveles de Madurez**																	
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI																		
Políticas																		
Procedimientos																		
Capacitación del Personal																		
Gestión del Proceso																		

Número de Casillas Puntuadas																		
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5		
Puntos obtenidos por cada columna (n° de casillas x valor)																		
Resultado Final																		

Gracias por responder la Hoja de Evaluación

ANEXO C

RESPUESTAS A LA HOJA DE EVALUACIÓN

Proceso: Evaluar Riesgos

Descripción del Proceso: La evaluación de riesgos es el conjunto de pasos secuenciales, lógicos y sistemáticos para identificar, valorar y manejar los riesgos asociados a los procesos del Área de TI, los cuales ejecutados en forma organizada le permiten encontrar soluciones reales a los riesgos detectados.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Evaluar Riesgos																		
Parámetros	**Niveles de Madurez**																	
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI								X										
Políticas					X													
Procedimientos							X											
Capacitación del Personal								X										
Gestión del Proceso					X													

Número de Casillas Puntuadas					2		1	2										
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5		
Puntos obtenidos por cada columna (n° de casillas x valor)	0				2,8		2	4,8								9,6		
Resultado Final																1,92		

Gracias por responder la Hoja de Evaluación

Proceso: Evaluar Riesgos

Descripción del Proceso: La evaluación de riesgos es el conjunto de pasos secuenciales, lógicos y sistemáticos para identificar, valorar y manejar los riesgos asociados a los procesos del Área de TI, los cuales ejecutados en forma organizada le permiten encontrar soluciones reales a los riesgos detectados.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Evaluar Riesgos																			
Parámetros	**Niveles de Madurez**																		
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI				X															
Políticas			X																
Procedimientos					X														
Capacitación del Personal				X															
Gestión del Proceso					X														

Número de Casillas Puntuadas			1	2	2														
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5			
Puntos obtenidos por cada columna (n° de casillas x valor)	0			2	2,8											4,8			
Resultado Final																0,96			

Gracias por responder la Hoja de Evaluación

Proceso: Evaluar Riesgos

Descripción del Proceso: La evaluación de riesgos es el conjunto de pasos secuenciales, lógicos y sistemáticos para identificar, valorar y manejar los riesgos asociados a los procesos del Área de TI, los cuales ejecutados en forma organizada le permiten encontrar soluciones reales a los riesgos detectados.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Evaluar Riesgos																		
Parámetros	**Niveles de Madurez**																	
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI						X												
Políticas	X																	
Procedimientos					X													
Capacitación del Personal				X														
Gestión del Proceso					X													

Número de Casillas Puntuadas	1			1	2	1												
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5		
Puntos obtenidos por cada columna (n° de casillas x valor)	0			1	2,8	1,7										5,5		
Resultado Final																1,1		

Gracias por responder la Hoja de Evaluación

Proceso: Evaluar Riesgos

Descripción del Proceso: La evaluación de riesgos es el conjunto de pasos secuenciales, lógicos y sistemáticos para identificar, valorar y manejar los riesgos asociados a los procesos del Área de TI, los cuales ejecutados en forma organizada le permiten encontrar soluciones reales a los riesgos detectados.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Evaluar Riesgos																			
Parámetros	**Niveles de Madurez**																		
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI						X													
Políticas			X																
Procedimientos							X												
Capacitación del Personal			X																
Gestión del Proceso					X														

Número de Casillas Puntuadas			2		1	1	1												
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5			
Puntos obtenidos por cada columna (n° de casillas x valor)	0				1.4	1,7	2									5,1			
Resultado Final																1,02			

Gracias por responder la Hoja de Evaluación

Proceso: Evaluar Riesgos

Descripción del Proceso: La evaluación de riesgos es el conjunto de pasos secuenciales, lógicos y sistemáticos para identificar, valorar y manejar los riesgos asociados a los procesos del Área de TI, los cuales ejecutados en forma organizada le permiten encontrar soluciones reales a los riesgos detectados.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Evaluar Riesgos																		
Parámetros	**Niveles de Madurez**																	
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI								X										
Políticas						X												
Procedimientos								X										
Capacitación del Personal					X													
Gestión del Proceso							X											

Número de Casillas Puntuadas					1	1	1	2										
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5		
Puntos obtenidos por cada columna (n° de casillas x valor)	0				1,4	1,7	2	4.8								9,9		
Resultado Final																1,98		

Gracias por responder la Hoja de Evaluación

Proceso: Administrar Cambios

Descripción del Proceso: La administración de cambio es el conjunto de acciones que se deben llevar a cabo formalmente y controladamente para todos los cambios, sean estos de infraestructura o aplicaciones. Los cambios de procedimientos, procesos, sistema deben ser registrados, evaluados y autorizados para su implementación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Administrar cambios																		
Parámetros	**Niveles de Madurez**																	
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI									X									
Políticas					X													
Procedimientos								X										
Capacitación del Personal						X												
Gestión del Proceso							X											

Número de Casillas Puntuadas					1	1	1	1	1									
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5		
Puntos obtenidos por cada columna (n° de casillas x valor)					1,4	1,7	2	2,4	2,7							10,2		
Resultado Final																2,04		

Gracias por responder la Hoja de Evaluación

Proceso: Administrar Cambios

Descripción del Proceso: La administración de cambio es el conjunto de acciones que se deben llevar a cabo formalmente y controladamente para todos los cambios, sean estos de infraestructura o aplicaciones. Los cambios de procedimientos, procesos, sistema deben ser registrados, evaluados y autorizados para su implementación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Administrar cambios																				
Parámetros	**Niveles de Madurez**																			
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**			
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**			
Relevancia del Proceso de TI								X												
Políticas		X																		
Procedimientos					X															
Capacitación del Personal			X																	
Gestión del Proceso					X															

Número de Casillas Puntuadas		1	1		2			1												
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5				
Puntos obtenidos por cada columna (n° de casillas x valor)					2,8			2,4								5,2				
Resultado Final																1,04				

Gracias por responder la Hoja de Evaluación

Proceso: Administrar Cambios

Descripción del Proceso: La administración de cambio es el conjunto de acciones que se deben llevar a cabo formalmente y controladamente para todos los cambios, sean estos de infraestructura o aplicaciones. Los cambios de procedimientos, procesos, sistema deben ser registrados, evaluados y autorizados para su implementación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Administrar cambios																		
Parámetros	**Niveles de Madurez**																	
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI									X									
Políticas					X													
Procedimientos									X									
Capacitación del Personal					X													
Gestión del Proceso								X										

Número de Casillas Puntuadas					2			1	2									
Valor Asignado a la Casilla	0			1	1,4		2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5		
Puntos obtenidos por cada columna (n° de casillas x valor)					2,8			2,4	5,4							10,6		
Resultado Final																2,12		

Gracias por responder la Hoja de Evaluación

Proceso: Administrar Cambios

Descripción del Proceso: La administración de cambio es el conjunto de acciones que se deben llevar a cabo formalmente y controladamente para todos los cambios, sean estos de infraestructura o aplicaciones. Los cambios de procedimientos, procesos, sistema deben ser registrados, evaluados y autorizados para su implementación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Administrar cambios																		
Parámetros	**Niveles de Madurez**																	
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI						X												
Políticas		X																
Procedimientos						X												
Capacitación del Personal		X																
Gestión del Proceso						X												

Número de Casillas Puntuadas		2				3												
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5		
Puntos obtenidos por cada columna (n° de casillas x valor)						5,1										5,1		
Resultado Final																1,02		

Gracias por responder la Hoja de Evaluación

Proceso: Administrar Cambios

Descripción del Proceso: La administración de cambio es el conjunto de acciones que se deben llevar a cabo formalmente y controladamente para todos los cambios, sean estos de infraestructura o aplicaciones. Los cambios de procedimientos, procesos, sistema deben ser registrados, evaluados y autorizados para su implementación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Administrar cambios																			
Parámetros	**Niveles de Madurez**																		
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI				X															
Políticas				X															
Procedimientos					X														
Capacitación del Personal			X																
Gestión del Proceso						X													

Número de Casillas Puntuadas			1	2	1	1													
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5			
Puntos obtenidos por cada columna (n° de casillas x valor)				2	1,4	1,7										5,1			
Resultado Final																1,02			

Gracias por responder la Hoja de Evaluación

Proceso: Administrar Instalaciones

Descripción del Proceso: El proceso Administrar Instalaciones requiere de instalaciones bien diseñadas y bien administradas, para obtener la protección de los equipos y del personal. El proceso de Administrar Instalaciones incluye la definición de los requerimientos físicos del área de sistemas, la selección de instalaciones apropiadas y el diseño de procesos efectivos para administrar el acceso físico.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Administrar Instalaciones																		
Parámetros	**Niveles de Madurez**																	
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI											X							
Políticas								X										
Procedimientos										X								
Capacitación del Personal								X										
Gestión del Proceso												X						

Número de Casillas Puntuadas								2		1	1	1						
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5		
Puntos obtenidos por cada columna (n° de casillas x valor)								4,8		3	3.4	3,7				14,9		
Resultado Final																2,98		

Gracias por responder la Hoja de Evaluación

Proceso: Administrar Instalaciones

Descripción del Proceso: El proceso Administrar Instalaciones requiere de instalaciones bien diseñadas y bien administradas, para obtener la protección de los equipos y del personal. El proceso de Administrar Instalaciones incluye la definición de los requerimientos físicos del área de sistemas, la selección de instalaciones apropiadas y el diseño de procesos efectivos para administrar el acceso físico.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Administrar Instalaciones																			
Parámetros	**Niveles de Madurez**																		
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**			
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**			
Relevancia del Proceso de TI										X									
Políticas										X									
Procedimientos											X								
Capacitación del Personal							X												
Gestión del Proceso												X							

Número de Casillas Puntuadas							1			2	1	1							
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5			
Puntos obtenidos por cada columna (n° de casillas x valor)							2			6	3,4	3,7				15,1			
Resultado Final																2,98			

Gracias por responder la Hoja de Evaluación

Proceso: Administrar Instalaciones

Descripción del Proceso: El proceso Administrar Instalaciones requiere de instalaciones bien diseñadas y bien administradas, para obtener la protección de los equipos y del personal. El proceso de Administrar Instalaciones incluye la definición de los requerimientos físicos del área de sistemas, la selección de instalaciones apropiadas y el diseño de procesos efectivos para administrar el acceso físico.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Administrar Instalaciones																		
Parámetros	**Niveles de Madurez**																	
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI									X									
Políticas									X									
Procedimientos								X										
Capacitación del Personal							X											
Gestión del Proceso							X											

Número de Casillas Puntuadas							2	1	2									
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5		
Puntos obtenidos por cada columna (n° de casillas x valor)							4	2,4	5,4							11,8		
Resultado Final																2,36		

Gracias por responder la Hoja de Evaluación

Proceso: Administrar Instalaciones

Descripción del Proceso: El proceso Administrar Instalaciones requiere de instalaciones bien diseñadas y bien administradas, para obtener la protección de los equipos y del personal. El proceso de Administrar Instalaciones incluye la definición de los requerimientos físicos del área de sistemas, la selección de instalaciones apropiadas y el diseño de procesos efectivos para administrar el acceso físico.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Administrar Instalaciones																		
Parámetros	**Niveles de Madurez**																	
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI											X							
Políticas										X								
Procedimientos												X						
Capacitación del Personal								X										
Gestión del Proceso											X							

Número de Casillas Puntuadas								1		1	2	1						
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5		
Puntos obtenidos por cada columna (n° de casillas x valor)								2,4		3	6,8	3,7				15,9		
Resultado Final																3,18		

Gracias por responder la Hoja de Evaluación

Proceso: Administrar Instalaciones

Descripción del Proceso: El proceso Administrar Instalaciones requiere de instalaciones bien diseñadas y bien administradas, para obtener la protección de los equipos y del personal. El proceso de Administrar Instalaciones incluye la definición de los requerimientos físicos del área de sistemas, la selección de instalaciones apropiadas y el diseño de procesos efectivos para administrar el acceso físico.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Administrar Instalaciones																		
Parámetros	**Niveles de Madurez**																	
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI									X									
Políticas							X											
Procedimientos								X										
Capacitación del Personal					X													
Gestión del Proceso									X									

Número de Casillas Puntuadas																		
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5		
Puntos obtenidos por cada columna (n° de casillas x valor)					1,4		2	2,4	5,4							11,2		
Resultado Final																2,24		

Gracias por responder la Hoja de Evaluación

Proceso: Garantizar la Seguridad de Sistemas

Descripción del Proceso: Garantizar la Seguridad de los Sistemas requiere de un proceso de Administración de Seguridad que permita mantener la integridad de la información y de proteger los activos de TI. Este proceso incluye establecer roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreo de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Garantizar la Seguridad de Sistemas																		
Parámetros	**Niveles de Madurez**																	
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI									X									
Políticas						X												
Procedimientos								X										
Capacitación del Personal						X												
Gestión del Proceso									X									

Número de Casillas Puntuadas						2		1	2									
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5		
Puntos obtenidos por cada columna (n° de casillas x valor)						3,4		2,4	5,4							11,2		
Resultado Final																2,24		

Gracias por responder la Hoja de Evaluación

Proceso: Garantizar la Seguridad de Sistemas

Descripción del Proceso: Garantizar la Seguridad de los Sistemas requiere de un proceso de Administración de Seguridad que permita mantener la integridad de la información y de proteger los activos de TI. Este proceso incluye establecer roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreo de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Garantizar la Seguridad de Sistemas																		
Parámetros	**Niveles de Madurez**																	
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI						X												
Políticas		X																
Procedimientos					X													
Capacitación del Personal				X														
Gestión del Proceso				X														

Número de Casillas Puntuadas		1		2	1	1												
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5		
Puntos obtenidos por cada columna (n° de casillas x valor)				2	1,4	1,7										5,1		
Resultado Final																1,02		

Gracias por responder la Hoja de Evaluación

Proceso: Garantizar la Seguridad de Sistemas

Descripción del Proceso: Garantizar la Seguridad de los Sistemas requiere de un proceso de Administración de Seguridad que permita mantener la integridad de la información y de proteger los activos de TI. Este proceso incluye establecer roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreo de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Garantizar la Seguridad de Sistemas																			
Parámetros	**Niveles de Madurez**																		
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**			
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**			
Relevancia del Proceso de TI				X															
Políticas				X															
Procedimientos						X													
Capacitación del Personal		X																	
Gestión del Proceso				X															

Número de Casillas Puntuadas		1		3		1													
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5			
Puntos obtenidos por cada columna (n° de casillas x valor)				3		1,7										4,7			
Resultado Final																0,94			

Gracias por responder la Hoja de Evaluación

Proceso: Garantizar la Seguridad de Sistemas

Descripción del Proceso: Garantizar la Seguridad de los Sistemas requiere de un proceso de Administración de Seguridad que permita mantener la integridad de la información y de proteger los activos de TI. Este proceso incluye establecer roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreo de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Garantizar la Seguridad de Sistemas																			
Parámetros	**Niveles de Madurez**																		
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**		
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**		
Relevancia del Proceso de TI					X													
Políticas		X																
Procedimientos						X												
Capacitación del Personal				X														
Gestión del Proceso					X													

Número de Casillas Puntuadas		1		1	2	1													
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5			
Puntos obtenidos por cada columna (n° de casillas x valor)				1	2,8	1,7										5,5			
Resultado Final																1,1			

Gracias por responder la Hoja de Evaluación

Proceso: Garantizar la Seguridad de Sistemas

Descripción del Proceso: Garantizar la Seguridad de los Sistemas requiere de un proceso de Administración de Seguridad que permita mantener la integridad de la información y de proteger los activos de TI. Este proceso incluye establecer roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreo de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados.

Completar la hoja de evaluación con una cruz (x), en los niveles que crea que se encuentre el proceso en el Área de TI.

El evaluador debe realizar una lectura previa de las características de los parámetros en cada nivel de madurez, para luego determinar la situación real que se encuentra ese parámetro en el proceso de TI evaluado.

Proceso: Garantizar la Seguridad de Sistemas																				
Parámetros	**Niveles de Madurez**																			
	Nivel 0			**Nivel 1**			**Nivel 2**			**Nivel 3**			**Nivel 4**			**Nivel 5**			
	No existe			**Ad-hoc**			**Conciencia**			**Definido**			**Formal**			**Optimizado**			
Relevancia del Proceso de TI								X												
Políticas					X															
Procedimientos									X											
Capacitación del Personal						X														
Gestión del Proceso								X												

Número de Casillas Puntuadas					1	1		2	1											
Valor Asignado a la Casilla	0			1	1,4	1,7	2	2,4	2,7	3	3,4	3,7	4	4,4	4,7	5				
Puntos obtenidos por cada columna (n° de casillas x valor)					1,4	1,7		4,8	2,7							10,6				
Resultado Final																2,12				

Gracias por responder la Hoja de Evaluación

ANEXO D

CONTROLES A EVALUAR

Proceso: Evaluar Riesgos

Nombre del Evaluador:

Puesto en la empresa:

Completar el siguiente cuestionario completando los campos para el proceso en cuestión.

Proceso: Evaluar Riesgos		
Controles a Evaluar	**Cumplimiento del Control**	**Observación**
Existe un marco referencial para la evaluación sistemática de riesgos.	Si ____ No___	
El marco de referencia incorpora los riesgos de información relevantes para el logro de los objetivos de la empresa.	Si ____ No___	
Existe una base que determine la forma en que deben ser manejados los riesgos en un nivel aceptable.	Si ____ No___	
El enfoque de evaluación de riesgos asegura la evaluación actualizada de riesgos a nivel global.	Si ____ No___	
El enfoque de evaluación de riesgos asegura la evaluación actualizada de riesgos a nivel específico de sistemas.	Si ____ No___	
Existen procedimientos de evaluación de riesgos que determinen los factores externo e internos de los riesgos identificados.	Si ____ No___	
Los procedimientos de evaluación de riesgos toman en consideración los resultados de las auditorías, inspecciones, e incidentes identificados.	Si ____ No___	
Existe documentación de evaluación de riesgos con la metodología que se usa para tal fin.	Si ____ No___	
Existe documentación de evaluación de riesgo que identifique las exposiciones significativas y los riesgos correspondientes	Si ____ No___	
Existe un enfoque cuantitativo y/o cualitativo (o combinado) formal para la identificación y medición de riesgos, amenazas y exposiciones.	Si ____ No___	
Se incluyen técnicas de probabilidad, frecuencia y análisis de amenazas en la identificación de riesgos.	Si ____ No___	
Se utilizan cálculos y otros métodos en la medición de riesgos, amenazas y exposiciones	Si ____ No___	
Existen procedimientos para el monitoreo de cambios en la actividad de procesamiento de sistemas.	Si ____ No___	
Los procedimientos de monitoreo de cambio determinan que los riesgos y exposición de los sistemas son ajustados oportunamente	Si ____ No___	
Existen procedimientos para el monitoreo y el mejoramiento continuos de la evaluación de riesgos.	Si ____ No___	
Los procedimientos para el mejoramiento de la evaluación de riesgos incluyen procesos para la creación de controles que mitiguen los riesgos.	Si ____ No___	
El personal asignado a evaluación de riesgos está adecuadamente calificado.	Si ____ No___	
Existe un Plan de acción contra riesgos.	Si ____ No___	

Proceso: Administrar Cambios		
Controles a Evaluar	**Cumplimiento del Control**	**Observación**
Existe y se utiliza una metodología para priorizar los requerimientos de los usuarios para cambios al sistema.	Si ____ No___	
Se consideran procedimientos de cambios de emergencia en los manuales de operaciones.	Si ____ No___	
El control de cambios es un procedimiento formal para los usuarios.	Si ____ No___	
El control de cambios es un procedimiento formal para los grupos de desarrollo.	Si ____ No___	
La bitácora de control de cambios asegura que todos los cambios mostrados fueron resueltos.	Si ____ No___	
El usuario está satisfecho con el resultado de los cambios solicitados.	Si ____ No___	
En la bitácora de control de cambio se especifica si el cambio trajo modificaciones en los programas y operaciones.	Si ____ No___	
En la bitácora de control de cambio se registra que los cambios hayan sido llevados a cabo como fueron documentados.	Si ____ No___	
El proceso de cambios monitorea la mejora en el conocimiento del usuario con respecto al proceso.	Si ____ No___	
El proceso de cambios monitores la efectividad en el tiempo de respuesta y satisfacción del usuario con respecto al proceso.	Si ____ No___	

Proceso: Garantizar la Seguridad de Sistemas		
Controles a Evaluar	**Cumplimiento del Control**	**Observación**
Existe un plan de seguridad estratégico.	Si ____ No___	
El plan de seguridad estratégico proporciona una dirección y control centralizado sobre la seguridad de los sistemas de información.	Si ____ No___	
El plan de seguridad estratégico proporcione los requerimientos de seguridad del usuario como soporte.	Si ____ No___	
Se cuenta con una organización de seguridad centralizada responsable de asegurar el acceso apropiado a los recursos del sistema.	Si ___ No____	
Se cuenta con un esquema de clasificación de datos que indique que todos los recursos del sistema cuentan con un propietario responsable de su seguridad y contenido.	Si ____ No___	
Se cuenta con perfiles de seguridad de usuario.	Si ___ No____	
Se revisan regularmente los perfiles de usuarios con fines de re acreditación.	Si ___ No____	
La empresa brinda capacitación sobre seguridad de sistemas a sus empleados.	Si ____ No___	
El entrenamiento incluye concientización sobre seguridad de sistemas y responsabilidad de propietario.	Si ____ No__	
Se capacita sobre los requerimientos de protección contra virus o ataques maliciosos.	Si ____ No___	
Se cuenta con reportes de fallas a la seguridad y procedimientos formales de solución de problemas.	Si ___ No____	
Se cuenta con reportes de Intentos no autorizados de acceso al sistema.	Si ___ No____	
Se cuenta con reportes de Intentos no autorizados de acceso a los recursos del sistema.	Si ___ No____	
Se cuenta con reportes de Intentos no autorizados para consultar o modificar las definiciones y reglas de seguridad.	Si ___ No____	

Controles a Evaluar	Cumplimiento del Control	Observación
Se cuenta con reportes de privilegios de acceso a recursos por ID de usuario.	Si ___ No____	
Se cuenta con reportes de modificaciones autorizadas a las definiciones y reglas de seguridad.	Si ___ No____	
Se cuenta con reportes de accesos autorizados a los recursos.	Si ___ No____	
Se cuenta con reportes de cambio de estatus de la seguridad del sistema.	Si ___ No____	
Se cuenta con reportes de accesos a las tablas de parámetros de seguridad del sistema operativo.	Si ___ No____	
Existen módulos criptográficos y procedimientos de mantenimiento de llaves.	Si ___ No___	
Los procedimientos de mantenimiento de llaves son administrados de forma centralizada y si son utilizados para todas las actividades de acceso externo y de transmisión.	Si ____ No___	
Existen estándares de administración de llaves criptográfica para la actividad centralizada.	Si ____ No___	
Existen estándares de administración de llaves criptográfica para los usuarios.	Si ____ No___	
Los controles de cambios al software de seguridad son formales y consistentes con los estándares normales de desarrollo y mantenimiento de sistemas.	Si ____ No___	
Los mecanismos de autenticidad proveen el uso individual de datos de autenticación (Ej., passwords nunca son reutilizados).	Si ____ No___	
Los mecanismos de autenticidad realizan una autentificación múltiple (Ej., se utilizan dos o más mecanismos de autenticación diferentes).	Si ____ No___	
Los mecanismos de autenticación es basada en políticas (Ej., capacidad para especificar procedimientos de autenticación separados para eventos específicos).	Si ____ No___	
Los mecanismos de autenticación se realiza por demanda (Ej., habilidad para re-autenticar al usuario otras veces después de la autentificación inicial).	Si ____ No___	
El número de sesiones concurrentes correspondientes al mismo usuario están limitadas.	Si ___ No___	
Al ingresar al sistema, aparece un mensaje de advertencia preventivo en relación al uso adecuado del hardware, software o conexión.	Si ____ No___	
Al lograrse la sesión exitosamente, se despliega el historial de los intentos exitosos y fallidos de acceso a la cuenta del usuario.	Si ____ No___	
La política de password fuerza el cambio inicial de la Clave la primera vez de uso.	Si ____ No___	
La política de password contempla la longitud adecuada mínima del password.	Si ___ No__	
La política de password especifica la frecuencia mínima obligada para el cambio de password.	Si ___ No__	
La política de password realiza una verificación del password en la lista de valores no permitidos (Ej., verificación de diccionario).	Si ___ No__	
La política de password contempla una protección adecuada para los passwords de emergencia.	Si ___ No__	
El procedimiento formal para resolución de problemas de ID de usuario, se lo suspende después de 5 intentos de entrada fallidas.	Si ___ No____	
El procedimiento formal para resolución de problemas de ID de usuario incluye Fecha del último acceso y el número de intentos fallidos se despliega al usuario autorizado una vez ingresado.	Si ___ No____	
El procedimiento formal para resolución de problemas de ID de usuario contempla el tiempo de autenticación es limitado a 5 minutos, después del cual se concluye la sesión.	Si ___ No____	
El procedimiento formal para resolución de problemas de ID de usuario, informa al usuario de la suspensión, pero no la razón de la misma.	Si ___ No____	

Controles a Evaluar	Cumplimiento del Control	Observación
La políticas relacionadas con cargos sensitivos incluyen que empleados en estos puestos sensitivos que permanezcan alejados de la organización durante un periodo adecuado de tiempo cada año calendario (período de vacaciones; durante éste tiempo su user ID es suspendido; y la persona que reemplaza al empleado es instruida en el sentido que debe notificar a la administración si nota cualquier anormalidad relacionada con la seguridad).	Si ___ No____	
Se produce una rotación de personal involucrado en actividades sensitivas, sin previa notificación, se realiza de tiempo en tiempo.	Si ___ No____	
El hardware y software de seguridad, así como los módulos criptográficos, están protegidos contra la intromisión o divulgación.	Si ____ No___	
El acceso a los datos de seguridad así como la administración de la seguridad, datos de transacciones sensitivas, passwords y llaves criptográficas se limita a la base de la "necesidad de conocer"	Si ___ No____	
Se utilizan rutas confiables para transmitir información sensitiva no encriptada.	Si ___ No___	
Las medidas de control detectivo y preventivo han sido establecidas por la administración para prevenir y detectar virus de computador.	Si ___ No____	
Para reforzar la integridad de los valores electrónicos, la empresa posee de lectores de tarjetas protegido contra la destrucción, publicación o modificación de la información de la tarjeta. • La información de la tarjeta (PIN y demás información) se protege contra la divulgación de intruso	Si ___ No____	
En la empresa la información de la tarjeta (PIN y demás información) se protege contra la divulgación de intruso	Si ___ No____	

ANEXO E

TABLA DE PRIORIDAD

Tabla De Prioridad

Dominio	Proceso	Criterios de Información							Recursos de TI				
		Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Recursos Humanos	Sistemas Información	Tecnología	Instalaciones	Datos
Planeación y Organización													
PO1	Definir un Plan Estratégico de TI	P	S						✓	✓	✓	✓	✓
PO2	Definir la Arquitectura de Información	P	S	S	S					✓			✓
PO3	Determinar la dirección tecnológica	P	S								✓	✓	
PO4	Definir la Organización y Relaciones de TI	P	S						✓				
PO5	Manejar la Inversión en TI	P	P					S	✓	✓	✓	✓	
PO6	Comunicar las directrices gerenciales	P					S		✓				
PO7	Administrar Recursos Humanos	P	P						✓				
PO8	Asegurar el cumplir Requerimientos Externos	P					P	S	✓	✓			✓
PO9	Evaluar Riesgos	S	S	P	P	P	S	S	✓	✓	✓	✓	✓
PO10	Administrar proyectos	P	P						✓	✓	✓	✓	
PO11	Administrar Calidad	P	P		P			S	✓	✓			
Adquisición e Implementación													
AI1	Identificar Soluciones	P	S							✓	✓	✓	
AI2	Adquisición y Mantener Software de Aplicación	P	P		S		S	S		✓			
AI3	Adquirir y Mantener Arquitectura de TI	P	P		S						✓		
AI4	Desarrollar y Mantener Procedimientos relacionados con TI	P	P		S		S	S	✓	✓	✓	✓	
AI5	Instalar y Acreditar Sistemas	P			S	S			✓	✓	✓	✓	✓
AI6	Administrar Cambios	P	P		P	P		S	✓	✓	✓	✓	✓
Servicios y Soporte													
DS1	Definir niveles de servicio	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
DS2	Administrar Servicios de Terceros	P	P	S	S	S	S	S	✓	✓	✓	✓	✓

DS3	Administrar Desempeño y Capacidad	P	P			S				✓	✓	✓		
DS4	Asegurar Servicio Continuo	P	S			P			✓	✓	✓	✓	✓	
DS5	Garantizar la Seguridad de Sistemas			P	P	S	S	S	✓	✓	✓	✓	✓	
DS6	Identificar y Asignar Costos		P					P	✓	✓	✓	✓	✓	
DS7	Capacitar Usuarios	P	S						✓					
DS8	Asistir a los Clientes de TI	P							✓	✓				
DS9	Administrar la Configuración	P				S		S		✓	✓	✓		
DS10	Administrar Problemas e Incidentes	P	P			S			✓	✓	✓	✓	✓	
DS11	Administrar Datos				P			P					✓	
DS12	Administrar Instalaciones				P	P						✓		
DS13	Administrar Operaciones	P	P		S	S			✓	✓	✓	✓	✓	

Monitoreo

M1	Monitorear los procesos	P	S	S	S	S	S	S	✓	✓	✓	✓	✓	
M2	Evaluar lo adecuado del control Interno	P	P	S	S	S	S	S	✓	✓	✓	✓	✓	
M3	Obtener aseguramiento independiente	P	P	S	S	S	S	S	✓	✓	✓	✓	✓	
M4	Proveer auditoría independiente	P	P	S	S	S	S	S	✓	✓	✓	✓	✓	

Tabla 21: Tabla de Prioridad

ANEXO F

DIRECTRICES DE AUDITORIA

DIRECTRICES DE AUDITORIA [1]

- **EVALUAR RIESGOS**

Los objetivos de control tanto detallados como de alto nivel son auditados al:

Obtener un entendimiento a través de:

- **Entrevistas:**
  - Presidencia de la función de servicios de información
  - Personal seleccionado de la función de servicios de información
  - Personal seleccionado de administración de riesgos
  - Usuarios claves de los servicios de TI
- **Obteniendo:**
  - Políticas y procedimientos relacionados con la evaluación de riesgos
  - Documentos de evaluación de riesgos del negocio
  - Documentos de evaluación de riesgos operativos
  - Documentos de evaluación de riesgos de la función de servicios de información
  - Detalles de la base sobre la cual se miden los riesgos y la exposición a los riesgos
  - Expedientes de personal para personal seleccionado de evaluación de riesgos
  - Políticas de seguros que cubren el riesgo residual
  - Resultados de las opiniones de expertos
  - Revisiones de grupos especializados
  - Consulta de las bases de datos de administración de riesgos

Evaluar los controles:

- **Considerando sí:**
  - Existe un marco referencial para la evaluación sistemática de riesgos, incorporando los riesgos de información relevantes para el logro de los objetivos de la organización y formando una base para determinar la forma en la que los riesgos deben ser manejados a un nivel aceptable.
  - El enfoque de evaluación de riesgos asegura la evaluación actualizada regular de riesgos tanto a nivel global como a nivel específico de sistemas.
  - Existen procedimientos de evaluación de riesgos para determinar que los riesgos identificados incluyen factores tanto externos como internos y toman en

consideración los resultados de las auditorías, inspecciones, e incidentes identificados.

- Los objetivos de toda la organización están incluidos en el proceso de identificación de riesgos.
- Los procedimientos para el monitoreo de cambios en la actividad de procesamiento de sistemas determinan que los riesgos y exposición de los sistemas son ajustados oportunamente.
- Existen procedimientos para el monitoreo y el mejoramiento continuos de la evaluación de riesgos y procesos para la creación de controles que mitiguen los riesgos.
- La documentación de evaluación de riesgos incluye:
  - una descripción de la metodología de evaluación de riesgos
  - la identificación de exposiciones significativas y los riesgos correspondientes
  - los riesgos y exposiciones correspondientes considerados
- Se incluyen técnicas de probabilidad, frecuencia y análisis de amenazas en la identificación de riesgos.
- El personal asignado a evaluación de riesgos está adecuadamente calificado
- Existe un enfoque cuantitativo y/o cualitativo (o combinado) formal para la identificación y medición de riesgos, amenazas y exposiciones.
- Se utilizan cálculos y otros métodos en la medición de riesgos, amenazas y exposiciones
- El plan de acción contra riesgos es utilizado en la implementación de medidas apropiadas para mitigar los riesgos, amenazas y exposiciones.
- La aceptación del riesgo residual toma en cuenta:
  - la política organizacional
  - la identificación y medición de riesgos
  - la incertidumbre inherente al enfoque de evaluación de riesgos mismo
  - el costo y la efectividad de implementar salvaguardas y controles
- La cobertura de los seguros compensan el riesgo residual
- Existen propuestas cualitativas y/o cuantitativas formales para seleccionar las medidas de control que maximicen el retorno de la inversión
- Existe un balance entre las medidas de detección, prevención, corrección y recuperación utilizadas

- Existen procedimientos formales para comunicar el propósito de la medición de los controles

Evaluar la suficiencia:

- **Probando que:**
  - Se cumple con el marco referencial de evaluación de riesgos en cuanto a que las evaluaciones de riesgos con actualizadas regularmente para reducir el riesgo a un nivel aceptable.
  - La documentación de evaluación de riesgos cumple con el marco referencial de evaluación de riesgos y su documentación es preparada y mantenida apropiadamente.
  - La administración y el personal de la función de servicios de información tienen conocimiento y conciencia y están involucrados en el proceso de evaluación de riesgos
  - La administración comprende los factores relacionados con los riesgos y la probabilidad de amenazas
  - El personal relevante comprende y acepta formalmente el riesgo residual
  - Los reportes emitidos a la Presidencia para su revisión y acuerdo con los riesgos identificados y utilización en el monitoreo de actividades de reducción de riesgos sean oportunos
  - El enfoque utilizado para analizar los riesgos traiga como resultado una medición cuantitativa o cualitativa (o combinada)de la exposición al riesgo
  - Los riesgos, amenazas y exposiciones identificados por la administración y atributos relacionados con los riesgos sean utilizados para detectar cada ocurrencia de una amenaza específica.
  - El plan de acción contra riesgos es actual e incluye controles económicos y medidas de seguridad para mitigar la exposición al riesgo
  - Se han priorizado los riesgos desde el más alto hasta el más bajo y existe una respuesta apropiada para cada riesgo:
    - control planeado preventivo de mitigación.
    - control secundario detectivo
    - control terciario correctivo
  - Los escenarios de riesgo versus los controles están documentados, actualizados y comunicados al personal apropiado

- Existe suficiente cobertura de seguros con respecto al riesgo residual aceptado y que éste es considerado contra varios escenarios de amenaza, incluyendo:
    - incendio, inundaciones, terremotos, tornados, terrorismo y otros desastres naturales no predecibles
    - violaciones a las responsabilidades fiduciarias del empleado
    - interrupción del negocio, pérdidas de ingresos, pérdida de clientes, etc.
    - otros riesgos no cubiertos generalmente por la tecnología de información y planes de riesgo/continuidad del Negocio

Comprobar el riesgo de los objetivos de control no alcanzados:

- **Llevando a cabo:**
    - Benchmarking del marco referencial de evaluaciones de riesgos contra organizaciones similares o estándares internacionales de la industria considerados como buenas prácticas.
    - Una revisión detallada del enfoque de evaluación de riesgos utilizado para identificar, medir y mitigar los riesgos a un nivel aceptable de riesgo residual

- **Identificando:**
    - Riesgos no identificados
    - Riesgos que no hayan sido medidos
    - Riesgos no considerados/administrados a un nivel aceptable
    - Evaluaciones de riesgos inoportunas y/o evaluaciones de riesgos con información desactualizada
    - Medidas incorrectas cuantitativas y/o cualitativas de riesgos, amenazas y exposiciones
    - Planes de acción contra riesgos que no aseguren controles económicos y medidas de seguridad
    - Falta de aceptación formal del riesgo residual
    - Cobertura de seguros inadecuada

- **ADMINISTRAR CAMBIOS**

Los objetivos de control tanto detallados como de alto nivel son auditados al:
Obtener un entendimiento a través de:

- **Entrevistas:**
  - Director de TI
  - Administración de la función de servicios de información
  - Administración de desarrollo de sistemas, aseguramiento de la calidad del control de cambios, operaciones y seguridad
  - Administración de usuarios seleccionada involucrada en el diseño y utilización de aplicaciones de sistemas de información
- **Obteniendo:**
  - Políticas y procedimientos organizacionales relacionadas con: planeación de sistemas de información, control de cambios, seguridad y ciclo de vida de desarrollo de sistemas
  - Políticas y procedimientos de la función de servicios de sistemas de información relacionadas con: metodología formal del ciclo de vida de desarrollo de sistemas, estándares de seguridad, aseguramiento independiente de la calidad, implementación, distribución, mantenimiento, cambios de emergencia, liberación de software y control de versiones del sistema.
  - Plan de desarrollo de aplicaciones
  - Formato y bitácora de requisiciones de control de cambios
  - Contratos con proveedores relacionados con servicios de desarrollo de aplicación

Evaluar los controles:
- **Considerando sí:**
  - Existe y se utiliza una metodología para priorizar los requerimientos de los usuarios para cambios al sistema
  - Se consideran procedimientos de cambios de emergencia en los manuales de operaciones
  - El control de cambios es un procedimiento formal tanto para los usuarios como para los grupos de desarrollo
  - La bitácora de control de cambios asegura que todos los cambios mostrados fueron resueltos

- El usuario está satisfecho con el resultado de los cambios solicitados - oportunidad y costos
- Para una selección de cambios en la bitácora de control de cambios:
    - el cambio trajo como resultado modificaciones en los programas y operaciones
    - los cambios hayan sido llevados a cabo como fueron documentados
    - la documentación actual refleja el ambiente modificado
- El proceso de cambios es monitoreado en cuanto a mejoras en el conocimiento, efectividad en el tiempo de respuesta y satisfacción del usuario con respecto al proceso
- El mantenimiento al sistema de Intercambio de red privada (Private Branch Exchange - PBX) se incluye en los procedimientos de control de cambios

Evaluar la suficiencia:

- **Probando que:**
    - Para una muestra de cambios, la administración ha aprobado los siguientes puntos:
        - solicitud de cambios
        - especificación del cambio
        - acceso al programa fuente
        - finalización del cambio por parte del programador
        - solicitud para mover el programa fuente al ambiente de prueba
        - finalización de pruebas de aceptación
        - solicitud de compilación y paso a producción
        - determinación y aceptación del impacto general y específico
        - desarrollo de un proceso de distribución
    - La revisión de la documentación de control de cambios en cuanto a la inclusión de:
        - fecha del cambio solicitado
        - persona(s) que lo solicitan
        - solicitud aprobada de cambios
        - aprobación del cambio realizado - función de servicios de información
        - aprobación del cambio realizado – usuarios

• fecha de actualización de documentación

• fecha de paso a producción

• aprobación del cambio por parte de aseguramiento de la calidad

• aceptación por parte de operaciones

- Los tipos de análisis de cambios realizados al sistema para la identificación de tendencias
- La evaluación de la adecuación de las librerías de la función de servicios de información y la determinación de la existencia de niveles de código base para prevenir la regresión de errores
- Existen procedimientos para verificar el código sin modificar y modificado para establecer los cambios realizados
- La bitácora de control de cambios asegura que todos los cambios fueron resueltos a satisfacción de los usuarios y que no se llevaron a cabo cambios que no hayan sido registrados en la bitácora
- Los usuarios tienen conciencia y conocimiento de la necesidad de procedimientos formales de control de cambios
- El proceso de reforzamiento del personal asegura el cumplimiento de los procedimientos de control de cambios

- **Llevando a cabo:**
  - Mediciones ("Benchmarking") de la administración de control de cambios contra organizaciones similares o apropiados estándares internacionales reconocidos como buenas prácticas de la industria
  - Para sistemas seleccionados de la función de servicios de información:

    • una verificación en cuanto a si la documentación determina el requerimiento o si el cambio del sistema ha sido aprobado y priorizado por parte de la administración de las áreas usuarias afectadas y el proveedor deservicios

    • la confirmación de la existencia y adecuación de evaluación del impacto en formas de control de cambios

    • la obtención del conocimiento del cambio a través de un acuse de recibo de solicitud de cambios de la función de servicios de información

    • la asignación del cambio a los recursos apropiados de desarrollo

    • la adecuación de los sistemas y los planes de prueba de los usuarios y sus resultados

• la migración formal de prueba a producción vía grupo de aseguramiento de la calidad

• la actualización de los manuales de usuario y de operación para reflejar el cambio

• la distribución de la nueva versión a los usuarios apropiados

- **Identificando:**
  - Para una selección de cambios de información que:

    • sólo se llevaron a cabo cambios aprobados

    • todos los cambios han sido considerados

    • las librerías actuales (fuente y objeto) reflejan los cambios más recientes

    • las variaciones en el procedimiento de control de cambios son registradas y consideradas entre:

      • aplicaciones adquiridas e internas

      • software de aplicación y de sistemas

      • tratamiento del control de cambios por parte del proveedor.

➢ GARANTIZAR LA SEGURIDAD DE SISTEMAS

Los objetivos de control tanto detallados como de alto nivel son auditados al:

Obtener un entendimiento a través de:

- **Entrevistas:**
  - Oficial de seguridad Senior de la organización
  - Administración de la seguridad y presidencia de TI
  - Administrador de la base de datos de TI
  - Administrador de la seguridad de TI
  - Administración de desarrollo de aplicaciones de TI
- **Obteniendo:**
  - Políticas y procedimientos globales para la organización referentes a la seguridad y el acceso de los sistemas de información
  - Políticas y procedimientos de TI relacionadas con: seguridad y acceso a los sistemas de información
  - Políticas y procedimientos relevantes, así como requerimientos de seguridad legales y regulatorios de los sistemas de

- información (por ejemplo, leyes, regulaciones, lineamientos/guías, estándares de la industria) incluyendo:
    - procedimientos de administración de cuentas de usuario.
    - política de seguridad del usuario o de protección de la información
    - estándares relacionados con el comercio electrónico
    - esquema de clasificación de datos
    - inventario de software de control de acceso
    - plano de los edificios/cuartos que contienen recursos de sistemas de información
    - inventario o esquema de los puntos de acceso físico a los recursos de sistemas de información (por ejemplo, módems, líneas telefónicas y terminales remotas)
    - procedimientos de control de cambios de software de seguridad
    - procedimientos de seguimiento, solución y escalamiento de problemas
    - reportes de violaciones a la seguridad y procedimientos de revisión administrativa
    - inventario de dispositivos de encriptación de datos y de estándares de encriptación
    - lista de los proveedores y clientes con acceso a los recursos del sistema
    - lista de los proveedores de servicios utilizados en la transmisión de datos
    - prácticas de administración de redes relacionadas con pruebas continuas de seguridad
    - copias de los contratos de los proveedores de servicios de transmisión de datos
    - copias de documentos firmados por lo usuarios relacionados con seguridad y concientización
    - contenido del material de entrenamiento de seguridad para nuevos empleados
    - reportes de auditoría de auditores externos, proveedores de servicios como terceras partes y dependencias
      gubernamentales relacionadas con la seguridad de los sistemas de información

Evaluar los controles:

- **Considerando sí:**
    - Se cuenta con un plan de seguridad estratégico que proporcione una dirección y control centralizados sobre la seguridad delos sistemas de información, así como requerimientos de seguridad de usuario, como soporte
    - Se cuenta con una organización de seguridad centralizada responsable de asegurar el acceso apropiado a los recursos del sistema
    - Se cuenta con un esquema de clasificación de datos en operación que indique que todos los recursos del sistema cuentan con un propietario responsable de su seguridad y contenido
    - Se cuenta con perfiles de seguridad de usuario que representen "los menos accesos requeridos" y que muestren revisiones regulares a los perfiles por parte de la administración con fines de reacreditación
    - El entrenamiento de los empleados incluye un conocimiento y conciencia sobre seguridad, las responsabilidades de los propietarios y los requerimientos de protección contra virus
    - Se cuenta con reportes de fallas a la seguridad y procedimientos formales de solución de problemas. Estos reportes deberán incluir:
        - intentos no autorizados de acceso al sistema (signon)
        - intentos no autorizados de acceso a los recursos del sistema
        - intentos no autorizados para consultar o modificar las definiciones y reglas de seguridad
        - privilegios de acceso a recursos por ID de usuario
        - modificaciones autorizadas a las definiciones y reglas de seguridad
        - accesos autorizados a los recursos (seleccionados por usuario o recurso)
        - cambio de estatus de la seguridad del sistema
        - accesos a las tablas de parámetros de seguridad del sistema operativo
    - Existen módulos criptográficos y procedimientos de mantenimiento de llaves, si éstos son administrados centralizadamente y si son utilizados para todas las actividades de acceso externo y de transmisión

- Existen estándares de administración de llaves criptográfica tanto para la actividad centralizada como para la de los usuarios
- Los controles de cambios al software de seguridad son formales y consistentes con los estándares normales de desarrollo y mantenimiento de sistemas
- Los mecanismos de autenticidad en uso proveen las siguientes facilidades:
  - uso individual de datos de autenticación (Ej., passwords nunca son reutilizados)
  - autentificación múltiple (Ej., se utilizan dos o más mecanismos de autenticación diferentes)
  - autenticación basada en políticas (Ej., capacidad para especificar procedimientos de autenticación separados para eventos específicos)
  - Autenticación por demanda (Ej., habilidad para re-autenticar al usuario otras veces después de la autentificación inicial)
- El número de sesiones concurrentes correspondientes al mismo usuario están limitadas
- Al ingresar al sistema, aparece un mensaje de advertencia preventivo en relación al uso adecuado del hardware, software o conexión.
- Se despliega una pantalla de advertencia antes de completar la entrada para informar al lector que los accesos no autorizados podrían causar responsabilidades legales
- Al lograrse la sesión exitosamente, se despliega el historial de los intentos exitosos y fallidos de acceso a la cuenta del usuario
- La política de password incluye:
  - Forzar el cambio inicial de password la primera vez de uso
  - longitud adecuada mínima del password
  - la frecuencia obligada mínima de cambio de password
  - verificación del password en la lista de valores no permitidos (Ej., verificación de diccionario)
  - protección adecuada para los passwords de emergencia
- El procedimiento formal para resolución de problemas incluye:
  - ID de usuario suspendido después de 5 intentos de entrada fallidos
  - Fecha del último acceso y el número de intentos fallidos se despliega al usuario autorizado una vez ingresado

• El tiempo de autenticación se limita a 5 minutos, después del cual se concluye la sesión

• Se le informa al usuario la suspensión, pero no la razón de la misma

- Los procedimientos de marcación telefónica incluyen autenticación basada en token o dial-back, cambios frecuentes del número telefónico, firewalls de hardware y software para restringir el acceso a los activos y cambios frecuentes de las claves de acceso y desactivación de las claves de acceso de los empleados temporales
- Los métodos de control por ubicación física se utilizan para aplicar restricciones adicionales a las ubicaciones específicas
- El acceso al servicio de correo de voz y el sistema PBX está controlado con los mismos controles físicos y lógicos de los sistemas computacionales
- El refuerzo a las políticas relacionadas con cargos sensitivos, incluyen:

  • se les pide a los empleados en puestos sensitivos que permanezcan alejados de la organización durante un periodo adecuado de tiempo cada año calendario (período de vacaciones; durante éste tiempo su user ID es suspendido; y la persona que reemplaza a el empleado es instruido en el sentido que debe notificar a la administración si nota cualquier anormalidad relacionada con la seguridad)

  • la rotación de personal involucrado en actividades sensitivas, sin previa notificación, se realiza de tiempo en tiempo
- El hardware y software de seguridad, así como los módulos criptográficos, están protegidos contra la intromisión o divulgación, el acceso se limita a la base de la "necesidad de conocer"
- El acceso a los datos de seguridad así como la administración de la seguridad, datos de transacciones sensitivas, passwords y llaves criptográficas se limita a la base de la "necesidad de conocer"
- Se utilizan rutas confiables para transmitir información sensitiva no encriptada
- Para evitar la negación del servicio por ataques con faxes basura, se toman medidas de seguridad como:

  • evitar la publicación de números de fax fuera de la organización en la base de "necesidad de conocer"

  • las líneas de fax utilizadas para solicitudes del negocio no se utilizan con otros fines

- Las medidas de control detectivo y preventivo han sido establecidas por la administración para prevenir y detectar virus de computador
- Para reforzar la integridad de los valores electrónicos, se toman las medidas:
  - facilidades de lector de tarjeta protegido contra la destrucción, publicación o modificación de la información de la tarjeta
  - la información de la tarjeta (PIN y demás información) se protege contra la divulgación de intruso
  - se evita la falsificación de las tarjetas
- Para reforzar la protección de las facilidad de seguridad, se toman medidas:
  - el proceso de identificación y autenticación requiere ser repetido después de un cierto periodo de inactividad un botón de bloqueo del sistema, un botón para forzar la salida o una secuencia de salida se puede activar cuando la terminal se deja desatendida

Evaluar la suficiencia:

- **Probando que:**
  - TI cumple con los estándares de seguridad relacionados con:
    - autenticación y acceso
    - administración de perfiles de usuario y clasificación de la seguridad de datos
    - reportes y revisión gerencial de las violaciones e incidentes de seguridad
    - estándares de administración de llaves criptográficas
    - Detección, resolución y comunicación sobre virus
    - clasificación y propiedad de datos
  - Existen procedimientos para la requisición, establecimiento y mantenimiento del acceso de usuarios al sistema
  - Existen procedimientos para el acceso externo de recursos del sistema, por ejemplo, "logon", "ID", "password" o contraseña y "dial back"
  - Se lleva un inventario de los dispositivos de acceso al sistema para verificar su suficiencia
  - Los parámetros de seguridad del sistema operativo tienen como base estándares locales/del proveedor
  - Las prácticas de administración de seguridad de la red son comunicadas, comprendidas e impuestas

- Los contratos de los proveedores de acceso externo incluyen consideraciones sobre responsabilidades y procedimientos de seguridad
- Existen procedimientos de "logon" vigentes para sistemas, usuarios y para el acceso de proveedores externos
- Se emiten reportes de seguridad en cuanto a la oportunidad, precisión y respuesta gerencial a incidentes
- Existen llaves secretas para la transmisión
- Los procedimientos para la protección contra software malicioso incluyen:

• todo el software adquirido por la organización se revisa contra los virus antes de su instalación y uso

• existe una política por escrito sobre descargue de archivos, aceptación y uso de software, freeware y shareware yesta política está vigente

• el software para aplicaciones altamente sensibles está protegido por MAC (Messsage Authentication Code- Código de Autentificación de Mensajes) o firma digital, y se utilizan mecanismos, fallas de verificación para evitar el uso del software

• los usuarios tienen instrucciones para la detección y reportes de virus, como el desempeño lento o crecimiento misterioso de archivos

• existe una política y un procedimiento vigente para la verificación de disquetes obtenidos por fuera del programa de compra normal de la organización

- Los firewalls poseen por lo menos las siguientes propiedades:

• todo el tráfico de adentro hacia fuera y viceversa debe pasar por estos firewalls (esto no debe limitarse a los controles lógicos, debe reforzarse físicamente)

• sólo se permitirá el paso al tráfico autorizado, como se define en la política de seguridad local

• los firewalls por sí mismo es inmune a la penetración

• el tráfico de intercambio en el firewall se lleva a cabo en la capa de aplicación únicamente

• la arquitectura del firewall combina las medidas de control tanto a nivel de la red como de la aplicación

• la arquitectura del firewall refuerza la discontinuidad de un protocolo en la capa de transporte

• la arquitectura del firewall debe estar configurada de acuerdo a la "filosofía de arte mínimo"

• la arquitectura del firewall debe desplegar sólida autentificación para la administración y sus componentes

• la arquitecura del firewall oculta la estructura de la red interna

• la arquitectura del firewall provee una auditoría de todas las comunicaciones hacia o a través del sistema del firewall y activará alarmas cuando se detecte alguna actividad sospechosa

• el host de la organización, que provee el soporte para las solicitudes de entrada al servicio de las redes públicas, permanece fuera del firewall

• la arquitectura del firewall se defiende de los ataques directos (Ej., a través del monitoreo activo de la tecnología de reconocimiento de patrones y tráfico)

• todo código ejecutable se explora en busca de códigos maliciosos (Ej., virus, applets dañinos) antes de introducirse

Comprobar el riesgo de los objetivos de control no alcanzados:

- **Llevando a cabo:**
  - Mediciones ("Benchmarking") de la seguridad de los sistemas de información contra organizaciones similares o estándares internacionales apropiados reconocidos con mejores prácticas de la industria
  - Una revisión detallada de la seguridad de los sistemas de información, incluyendo evaluaciones de penetración de la seguridad física y lógica de los recursos computacionales y de comunicaciones, etc.
  - Entrevistas a los nuevos empleados para asegurar el conocimiento y la conciencia en cuanto a seguridad y en cuanto a las responsabilidades individuales, por ejemplo, confirmar la existencia de declaraciones de seguridad firmadas y el entrenamiento para nuevos empleados en cuanto a seguridad
  - Entrevistas a usuarios para asegurar que el acceso está determinado tomando como base la necesidad ("menor necesidad") y que la precisión de dicho acceso es revisada regularmente por la gerencia
- **Identificando:**
  - Accesos inapropiados por parte de los usuarios a los recursos del sistema

- Inconsistencias con el esquema o inventario de redes en relación con puntos de acceso faltantes, accesorios faltantes, etc.
- Deficiencias en los contratos en cuanto a la propiedad y responsabilidades relacionadas con la integridad y seguridad de los datos en cualquier punto de la transmisión entre el envío y la recepción
- Empleados no verificados como usuarios legítimos o empleados ya retirados que cuenten aún con acceso
- Requisiciones informales o no aprobadas de acceso a los recursos del sistema
- Software de monitoreo de redes que no indique a la administración de redes las fallas a la seguridad
- Defectos en los procedimientos de control de cambios del software de redes
- La no utilización de llaves secretas en los procedimientos de emisión/recepción de terceras partes
- Deficiencias en los protocolos para generación de llaves, almacenamiento de distribución, entrada, uso, archivo y protección
- La falta de software actualizado para la detección de virus o de procedimientos formales para prevenir, detectar, corregir y comunicar contaminaciones