AUDITORIA AL MÓDULO DE CONSULTA EXTERNA DEL SISTEMA DE INFORMACIÓN MEDULA DE LA EMPRESA COMPGENIOSS LTDA

ALCIDES DE JESÚS GIOVANNETTI CAHUANA
IRLETH KARINE FONSECA ZAMBRANO
JOSÉ LUIS REDONDO AGUILAR

ASESOR:

ING. TELMA BARRAZA OLAYA

UNIVERSIDAD DE LA COSTA
FACULTAD DE POSGRADO

ESPECIALIZACIÓN EN AUDITORIA A LOS SISTEMAS DE INFORMACIÓN
BARRANQUILLA ATLÁNTICO
2012

AUDITORIA AL MÓDULO DE CONSULTA EXTERNA DEL SISTEMA DE INFORMACIÓN MEDULA DE LA EMPRESA COMPGENIOSS LTDA

ALCIDES DE JESÚS GIOVANNETTI CAHUANA
IRLETH KARINE FONSECA ZAMBRANO
JOSÉ LUIS REDONDO AGUILAR

ASESOR:

ING. TELMA BARRAZA OLAYA

UNIVERSIDAD DE LA COSTA
FACULTAD DE POSGRADO

ESPECIALIZACIÓN EN AUDITORIA A LOS SISTEMAS DE INFORMACIÓN
BARRANQUILLA ATLÁNTICO
2012

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

JURADO

_____

JURADO

_____

PRESIDENTE DE JURADO

BARRANQUILLA ATLÁNTICO AGOSTO DE 2012

AGRADECIMIENTO

Los autores agradecen a Dios, que nos mantuvo a diario con nuestra salud e iluminó nuestros pensamientos en todas nuestras actividades para poder culminar nuestras metas propuestas.

A la Ingeniera TELMA BARRAZA, por su incansable dedicación y paciencia para transmitirnos los conocimientos necesarios para poder alcanzar nuestros logros.

A la universidad por tener presente la importancia de la formación profesional de la comunidad educativa, con la implantación de planes y programas para capacitar a la comunidad de la Costa Caribe en general y del mismo modo por las facilidades económicas de acceso a la educación superior.

DEDICATORIA

El autor dedica a Dios por dotarme de sabiduría y de la facilidad de adquisición de los conocimientos necesarios para vivir la vida y sobre todo para poder ser un gran profesional. Por brindarme una vida llena de oportunidades para ser alguien en la vida y también por permitirme compartir con todos mis familiares y amigos más allegados.

A mi padre: por apoyarme en cada proyecto de vida que deseo emprender, por inculcarme valores y principios, por el incondicional apoyo que constantemente me ofrece lo cual me motiva a seguir adelante día a día.

A mi madre, por regalarme la oportunidad de vivir y dedicarme tiempo, afecto, amor y crianza durante las etapas de mi vida, gracias su cariño siempre he sentido apoyo en mi vida.

Alcides Giovannetti Cahuana

DEDICATORIA

El autor dedica a Dios todo poderoso, quien está a mi lado a cada instante, por ser el dador de nuestras vidas e inteligencia y es quien nos conduce hacia el futuro.

A mis padres quienes con su cariño y esfuerzo me apoyaron para salir adelante.

A mis hermanos, y amigos que contribuyeron con su orientación para hacer posible este objetivo propuesto

A la Ingeniera Telma Barraza quien por sus importantes sugerencias y orientaciones nos permitió terminar muy satisfactoriamente nuestro proyecto, que hoy presentamos como el fruto de sus aportes.

Irleth Fonseca Zambrano

DEDICATORIA

El autor dedica a Dios, quien es la luz y mi camino en mi vida, por ser mi voz de aliento en los momentos difíciles y ser mi guía de felicidad y tranquilidad que llena mi vida, este es un triunfo se lo dedico todo a él, porque con Dios todo es posible en la vida.

Este triunfo se lo dedico a mis padres, quienes son los dos pilares de mi vida, quienes con su amor, esfuerzos y sacrificios, me han sacada adelante, esta meta se la debo todo a ellos. GRACIAS LOS AMO.

A mi hermana, abuelos y amigos que contribuyeron con su apoyo y cariño para hacer posible esta meta profesional.

A la Ingeniera Telma Barraza quien por sus importantes sugerencias y orientaciones nos permitió terminar muy satisfactoriamente nuestro proyecto de grado.

José Redondo Aguilar

RESUMEN

COMPGENIOSS LTDA. es una organización que tiene como actividad comercial el desarrollo de software a la medida, consultoría, asesorías y sistematización en general.

Esta organización optó por desarrollar un nuevo software llamado MEDULA, dedicado a la gestión hospitalaria el cual es un sistema de información para las instituciones prestadora de salud (IPS) en todos sus niveles de atención y complejidad que involucra el manejo integral de la gestión administrativa y asistencial. El aplicativo es soportado por una serie de módulos tales como: Urgencia, Hospitalización, Consulta externa, Historia clínica, Enfermería, Estadística y Facturación.

La organización es consciente de los posibles riesgos que pueden presentarse durante la implementación del software, con el fin de minimizar la materialización de posibles riesgos ha decidido brindar a sus actuales y futuros clientes un software de calidad, de allí nace la necesidad de realizar una auditoría al sistema de información MEDULA, específicamente al módulo de consulta externa. Esta auditoría consistió en realizar la evaluación y verificación de los controles, la integridad y confidencialidad de los datos, accesos y perfiles al sistema, interfaces y posibles errores o fallas del aplicativo, utilizando como Marco de Referencia COBIT 4.1 el cual se complementó con ISO 27002, ITIL V3, ISO 3100 obteniendo de ellos varios controles, procesos y métodos, con el propósito de identificar las debilidades y fortalezas soportadas en estas buenas prácticas.

ABSTRACT

COMPGENIOSS LTDA. is an organization whose business developing custom software, consulting, advisory and general systematization

This organization decided to develop a new software called MEDULA, dedicated to hospital management which is an information system for health care provider institutions (hcpi) at all levels of care and complexity involving the comprehensive of the administrative and care. The application is supported by a number of moduls such as: emergency, inpatient, outpatient, medical history, nursing, statistcs and billing.

The organization is aware of the potential risks that may arise during the implementation of the software, in order to minimize potential risks materializing has decided to provide its currents and future customers a quality software. There arise the need for an audit MEDULA information system, specifically the outpatient module. This audit was to conduct the evaluation and testing of controls, integrity and confidentiality of data, and access to the system profiles, interfaces and possible errors or failures of the application, using COBIT 4.1 framework which complement with ISO 27002, ITIL V3, ISO3100 obtaining them several controls processes and methods for the purpose of identifying the weaknesses and strengths in these best practices supported

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE GRÁFICOS

INTRODUCCIÓN

La empresa de hoy se centra en el plano económico soportada en gran medida por la evolución de los medios tecnológicos para facilitar sus procesos y mejorar su rendimiento. La información es considerada como el activo más importante dentro de una organización siendo irrelevante e irremplazable para la empresa, por esta razón debe encontrarse resguardada de una cantidad de riesgos que se podrían materializar.

La mejor forma de gestionar y proteger la información y la infraestructura que la soporta viene dada por los estándares denominados como “mejores prácticas” entre los cuales podemos resaltar COBIT, ITIL e ISO 27000. La ventaja de utilizar e implementar estos estándares es que se puede percibir de una forma sencilla que tan lejos o cerca está la compañía de una buena práctica, las cuales son un punto de partida importante a la hora de crear y proteger la información.

El presente trabajo tiene como finalidad realizar una auditoría al sistema de información MEDULA aplicando lineamientos denominados como mejores prácticas enfocado específicamente al marco de referencia COBIT para identificar posibles riesgos y proponer alternativas de solución a la empresa

1. INFORMACIÓN GENERAL DEL PROYECTO

Título: Auditoria Al Módulo de Consulta Externa Del Sistema De Información Medula De La Empresa CompGenioss LTDA.
Presentado por: Irleth Karine Fonseca Zambrano Alcides De Jesús Giovannetti Cahuana José Luis Redondo
Líneas de Investigación: Desarrollo Tecnológico e Innovación empresarial
Facultad: De Ingeniería
Correo electrónico: alcidesgiovannetti@hotmail.com irle0127@hotmail.com ing.joseluis.ra@hotmail.com
Duración del proyecto: 6 meses
Tipo de proyecto: Investigación Básica: _____ Investigación Aplicada: _____ Desarrollo Tecnológico o Experimental: ____**X**___

Tabla 1. Información general del proyecto

2. PLANTEAMIENTO DEL PROBLEMA

2.1 DESCRIPCIÓN DEL PROBLEMA

La información representa hoy día el activo más valioso dentro de una organización convirtiéndose de esta manera en irremplazable e imprescindible, por tal motivo las empresas dedican una cantidad considerable de tiempo y recursos en buscar la manera de llevar un control eficaz sobre la misma.

CompGenioss LTDA. es una empresa dedicada a la consultaría y gestión de sistemas, también incluyendo dentro de su portafolio de servicios la fabricación de software a la medida, uno de estos productos es un sistema de información llamado "MEDULA", dedicado a la gestión hospitalaria, siendo el hospital de SAN ONOFRE pionero en la adquisición del sistema de información MEDULA software que fue adquirido con el propósito de facilitar y coordinar de una manera más eficiente sus procesos hospitalarios como los son: contratos con las IPS y EPS, control de citas, consulta médica general, consulta especializada, atención por urgencias, entre muchos otros.

El proceso de adquirir un nuevo sistema de información es un asunto que debe realizarse de una manera controlada y siguiendo un conjunto de normas denominadas como mejores prácticas para garantizar excelentes resultados, CompGenioss LTDA. es consciente de esta situación así como de los posibles riesgos que pueden presentarse durante la transición, por tal motivo, con el fin de minimizar la materialización de posibles riesgos y decidido a brindar a sus actuales y futuros clientes un software de calidad optó por la realización de una auditoria al sistema de información MEDULA, específicamente al módulo de consulta externa, que pretende realizar la evaluación y verificación de los

controles, la integridad y confidencialidad de los datos, accesos y perfiles al sistema, interfaces y posibles errores o fallas del aplicativo, y sugerir alternativas de solución a fin de que se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

De lo anterior surge la siguiente pregunta:

¿Qué tipo de buenas prácticas serían las adecuadas a implementar, para que MEDULA, cumpla con lineamientos de controles que permitan minimizar los riesgos que se puedan presentar?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

- Realizar una auditoría al sistema de información MEDULA, en el módulo de consulta externa para identificar posibles riesgos y proponer alternativas de solución a la empresa

3.2 OBJETIVOS ESPECÍFICOS

- Realizar un análisis para determinar los riesgos que pueden presentarse e impiden el correcto funcionamiento del aplicativo MEDULA o comprometen la seguridad de la información.

- Verificar los controles existentes del módulo de consulta externa en el Software MEDULA y complementarlos.

- Determinar el nivel de madurez del aplicativo medula utilizando como apoyo el marco de referencia COBIT.

- Verificar la seguridad, la integridad, y el procesamiento de datos del aplicativo MEDULA

4. JUSTIFICACIÓN

En los procesos de negocios, que se llevan a cabo dentro de las unidades de una organización, se coordinan en función de los procesos de gestión básicos de planificación, ejecución y supervisión. El control que provee la auditoria es parte de dichos procesos y está integrado en ellos, permitiendo su funcionamiento adecuado y supervisando su comportamiento y aplicabilidad en cada momento, con lo que, constituye una herramienta útil para la gestión.

Con base en resultados obtenidos de pruebas realizadas al aplicativo MEDULA y en el tipo de competencia que enfrenta la empresa, se autorizó la aplicación de una auditoría al módulo de consulta externa del aplicativo MEDULA, con el fin de detectar amenazas de riesgos, que atenten contra el correcto funcionamiento del aplicativo, lo cual generaría pérdida económica e insatisfacción de la estrategia comercial a la organización, por tal motivo esta auditoría busca Prever y minimizar las causas que puedan hacer que estos Riesgos se materialicen.

Es conveniente señalar que otra razón de realizar la auditoría al aplicativo MEDULA, es para identificar oportunidades de mejora que le permitan ofrecer un mejor servicio a sus clientes, lo cual mejorara sustancialmente el desempeño de la empresa, garantizar un crecimiento y disponer de toda una gama de posibilidades para hacer frente de manera congruente a las demandantes condiciones del mercado.

Por tal razón es necesario efectuar una evaluación al módulo de consulta externa del software MEDULA de la organización CompGenioss con el fin de detectar las posibles causas de riesgos, detectar las falencias que estén afectando el proceso, así como también

aportar mejoras para hacer que el módulo de consulta externa sea mucho más seguro y confiable.

Se utilizaron estándares soportados en buenas prácticas, tales como, COBIT 4.1, ISO 27002, ITIL V3, obteniendo de ellos varios controles, procesos, y métodos de estos estándares. Enfocándonos principalmente a identificar y atacar las causas de riesgos que existen o que puedan presentarse durante el módulo de consulta externa del software MEDULA tratando de minimizar su ocurrencia e impacto.

5. MARCO DE REFERENCIA

Estos consisten en unas referencia breve al comienzo del estudio de la auditoria y está compuesto de conceptualizaciones del problema o de problemas conectados con el formulado por el equipo de auditores, define además términos empleados, teorías utilizadas, problemas estudiados, resultados obtenidos, explicaciones dadas, etc.

5.1 MARCO TEÓRICO

5.1.1 ESTÁNDARES DENOMINADOS "MEJORES PRACTICAS"

"Las mejores prácticas son directrices que permiten a las empresas modelar sus procesos para que se ajusten a sus propias necesidades, proporcionan a las empresas y/o organizaciones métodos utilizados para estandarizar procesos y administrar de una mejor manera los entornos de TI". [1]

5.1.1.1 CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY, COBIT

"COBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información (TI). – COBIT es la herramienta innovadora para el gobierno de TI.

1 Mejores prácticas de la auditoría en informática, Capítulo 3. Legislación informática, mejores prácticas y técnicas de auditoría informática

Este estándar es relativamente pequeño en tamaño, con el fin de ser práctico y responder, en la medida de lo posible, a las necesidades de negocio, manteniendo al mismo tiempo una independencia con respecto a las plataformas técnicas de TI adoptadas en una organización. El proporcionar indicadores de desempeño (normas, reglas, etc.), ha sido identificado como prioridad para las mejoras futuras que se realizarán al marco referencial".[2]

"COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados (Stakeholders). COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de la misma.

Los beneficios de implementar COBIT como marco de referencia de gobierno sobre TI incluyen:

- Mejor alineación, con base en su enfoque de negocios
- Una visión, entendible para la gerencia, de lo que hace TI
- Propiedad y responsabilidades claras, con base en su orientación a procesos
- Aceptación general de terceros y reguladores

2 Comité Directivo de COBIT y la Information Systems Audit and Control Foundation. Cobit Directrices De Auditoria. 2da Edición. 1998.

• Entendimiento compartido entre todos los Interesados, con base en un lenguaje común
• Cumplimiento de los requerimientos COSO para el ambiente de control de TI

Para que TI tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implementar un sistema de control interno o un marco de trabajo. El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:

• Estableciendo un vínculo con los requerimientos del negocio
• Organizando las actividades de TI en un modelo de procesos generalmente aceptado
• Identificando los principales recursos de TI a ser utilizados
• Definiendo los objetivos de control gerenciales a ser considerados

La orientación al negocio que enfoca COBIT consiste en alinear las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los dueños de los procesos de negocio y de TI.

El enfoque hacia procesos de COBIT se ilustra con un modelo de procesos, el cual subdivide TI en 34 procesos de acuerdo a las áreas de responsabilidad de planear, construir, ejecutar y monitorear, ofreciendo una visión de punta a punta de la TI. Los conceptos de arquitectura empresarial ayudan a identificar aquellos recursos esenciales para el éxito de los procesos, es decir, aplicaciones, información, infraestructura y personas.

En resumen, para proporcionar la información que la empresa necesita para lograr sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos agrupados de forma natural".[3]

5.1.1.2 INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY, ITIL

"Librería de Infraestructura de TI de la Oficina de Gobierno Gubernamental del Reino Unido (OGC).Un conjunto de lineamientos sobre la administración y procuración de servicios operativos de TI".[4]

"Hoy, las organizaciones dependen de las TI para satisfacer sus objetivos corporativos y sus necesidades de negocios, entregando valor a sus clientes. Para que esto ocurra de una forma gestionada, responsable y repetible, la empresa debe asegurar que los servicios recibidos de alta calidad de TI deben:

- Satisfacer las necesidades de la empresa y los requisitos de los usuarios.
- Cumplir con la legislación.
- Asignarse y entregarse de forma eficaz y eficiente.
- Revisarse y mejorarse de forma continua.

La gestión de servicios de TI se refiere a la planificación, aprovisionamiento, diseño, implementación, operación, apoyo y mejora de los servicios de TI que sean apropiados a las necesidades del negocio. ITIL proporciona un marco de trabajo de mejores prácticas integral, consistente y coherente para la gestión de servicios de TI y los procesos

3 IT Governance Institute. Cobit 4.1. 2007
4 Ibit.

relacionados, la promoción de un enfoque de alta calidad para el logro de la eficacia y eficiencia del negocio en la gestión de servicios de TI.

ITIL intenta respaldar mas no fijar los procesos de negocio de una organización. En este contexto, la OGC no aprueba el término "Cumplimiento con ITIL". El papel del marco de trabajo de ITIL es describir los enfoques, las funciones, los roles y procesos en los que las organizaciones pueden basar sus propias prácticas. El rol de ITIL es brindar orientación en el nivel organizacional más bajo que pueda aplicarse. Debajo de ese nivel, para implementar ITIL en una organización se requieren los conocimientos específicos de sus procesos de negocio para ajustar ITIL a fin de lograr una eficacia óptima"[5].

5.1.1.3 ISO/IEC 27002

"La norma publicó su primera edición en el año 2000 y actualizada en junio de 2005. Se puede clasificar como las mejores prácticas actuales en materia de sistemas de gestión de seguridad de la información. La BS 7799 original fue revisada y reeditada en septiembre de 2002. A menudo se utiliza ISO/IEC 27002 como un término genérico para describir lo que actualmente son dos documentos diferentes.

El objetivo del estándar ISO/IEC 27002:2005 es brindar información a los responsables de la implementación de seguridad de la información de una organización. Puede ser visto como una buena práctica para desarrollar y mantener normas de seguridad y prácticas de gestión en una organización para mejorar la fiabilidad en la seguridad de la información en las relaciones interorganizacionales. En él se definen las estrategias de 133 controles de seguridad organizados bajo 11 dominios. La norma subraya la Importancia de la gestión

5 IT Governance Institute. Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa.2008

del riesgo y deja claro que no es necesario aplicar cada parte, sino sólo aquellas que sean relevantes.

Los principios rectores en la norma ISO/IEC 27002:2005 son los puntos de partida para la implementación de seguridad de la información. Se basan en cualquiera de los requisitos legales o en las mejores prácticas generalmente aceptadas.

Las mediciones basadas en los requisitos legales son:

- La protección y la no divulgación de datos personales.
- Protección de la información interna.
- Protección de los derechos de propiedad intelectual.

Las mejores prácticas mencionadas en la norma incluyen:

- La política de seguridad de la información.
- Asignación de la responsabilidad de seguridad de la información.
- Escalamiento de problemas.
- Gestión de la continuidad del negocio."[6]

6 Ibit.

5.1.2 ISO/IEC 3100

“ISO 3100 fue preparada por el concejo de administración ISO Grupo de trabajo técnico sobre gestión de riesgos.

Esta norma internacional establece los principios y directrices de carácter genérico sobre la gestión del riesgo.

Puede ser utilizada por cualquier entidad pública, privada o comunitaria de la empresa, asociación, grupo o individuales. Por los tanto, esta norma internacional no es especifica de cualquier industria o sector.

Esta norma puede ser aplicada a lo largo de la vida de una organización, así como una amplia gama de actividades, incluidas las estrategias y decisiones, operaciones, procesos, funciones, proyectos, productos, servicios y activos.

Esta norma internacional puede ser aplicada a cualquier tipo de riesgo, cualquiera que sea su naturaleza, ya sea positivo o tener consecuencias negativas

Aunque esta norma proporciona directrices genéricas, no es la intención de promover la uniformidad de riesgo gestión en las organizaciones. El diseño y ejecución de planes de gestión de riesgos y marcos tendrá que tomar en cuenta las diversas necesidades de una organización específica, sus objetivos particulares, contexto, estructura, operaciones, procesos, funciones, proyectos, productos, servicios o activos específicos y practicas empleadas.

Se pretende que esta norma internacional se utilizará para armonizar la gestión del riesgo en existentes y las normas futuras. Proporciona un enfoque común a favor de normas que tratan sobre riesgos específicos y / o sectores, y no sustituyen a las normas."[7]

5.1.3 NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27005

"Esta norma proporciona directrices para la gestión del riesgo en la seguridad de la información en una organización, dando soporte particular a los requisitos de un sistema de gestión de seguridad de la información (SGSI) de acuerdo con la norma NTC-ISO/IEC 27001. Sin embargo, esta norma no brinda ninguna metodología específica para la gestión del riesgo, dependiendo por ejemplo del alcance de su SGSI, del contexto de la gestión del riesgo o del sector industrial. Se puede utilizar una variedad de metodologías existentes bajo la estructura descrita en esta norma para implementar los requisitos de un sistema de gestión de seguridad de la información.

Esta norma es pertinente para los directrices y el personal involucrado en la gestión del riesgo en la seguridad de la información dentro de una organización y cuando corresponda, para las partes externas que dar soporte a dichas actividades

Suministra directrices para la gestión del riesgo en la seguridad de la información. Esta norma brinda soporte a los conceptos generales que se especifican en la norma NTC-ISO/IEC 27001 y está diseñada para facilitar la implementación satisfactoria de la seguridad de la información con base en el enfoque de gestión del riesgo.

7 ISO/FDIS 3100: 2009 (E). La gestión de riesgos-principios y directrices.

Se aplica a todos los tipos de organizaciones (por ejemplo empresas comerciales, agencias del gobierno, organizaciones sin ánimo de lucro) que pretenden gestionar los riesgos que podrían comprometer la seguridad de la información de la organización."[8]

5.1.4 AUDITORIA DE SISTEMAS

"La auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y Seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones"[9]

"La auditoría en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software)."[10]

La naturaleza especializada de la auditoria de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de auditorías, requieren el desarrollo y la promulgación de Normas Generales para la Auditoria de los Sistemas de Información.

La auditoría de los sistemas de información se define como cualquier auditoria que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los

8 Norma Técnica Colombiana NTC-ISO/IEC 2700. Tecnología de la información, Técnicas de seguridad, Gestión del riesgo en la seguridad de la información. 2009-08-19
9 http://www.veeduriadistrital.gov.co/es/grupo/g285/web/Archivo2AS.pdf
10 http://www.gerencie.com/auditoria-de-sistemas-de-informacion.html

sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

La Auditoría de la seguridad en la informática abarca los conceptos de seguridad física y lógica. La seguridad física se refiere a la protección del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los albergan. El auditor informático debe contemplar situaciones de incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc.

Por su parte, la seguridad lógica se refiere a la seguridad en el uso de software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

El auditar la seguridad de los sistemas, también implica que se debe tener cuidado que no existan copias piratas, o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión de virus.

Los sistemas de auditoría comprenden estándares metodológicos, para la realización de una auditoria con sus correspondientes directrices, y así poder obtener resultados favorables frente a los diferentes obstáculos que un sistema de información posee en el momento de ser evaluado, y dirigir así a un proceso de nuevas correcciones y evaluaciones frente a la seguridad de la información. Por eso los sistemas de información y sus diferentes procesos se deben estar evaluando contrastantemente con estándares de auditoría.

5.1.5 SEGURIDAD INFORMÁTICA

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Podemos entender como seguridad un estado de cualquier tipo de información (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

- **Integridad:** La información sólo puede ser modificada por quien está autorizado y de manera controlada.
- **Confidencialidad:** La información sólo debe ser legible para los autorizados.
- **Disponibilidad:** Debe estar disponible cuando se necesita.
- **Irrefutabilidad (No repudio):** El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Dependiendo de las fuentes de amenaza, la seguridad puede dividirse en tres partes: seguridad física, seguridad ambiental y seguridad lógica.

En estos momentos la seguridad informática es un tema de dominio obligado por cualquier usuario de la Internet, para no permitir que su información sea comprometida

5.1.6 SQL SERVER

“SQL Server es un conjunto de objetos eficientemente almacenados. Los objetos donde se almacena la información se denominan tablas, y éstas a su vez están compuestas de filas y columnas. En el centro de SQL Server está el motor de SQL Server, el cual procesa los comandos de la base de datos. Los procesos se ejecutan dentro del sistema operativo y entienden únicamente de conexiones y de sentencias SQL.

SQL Server incluye herramientas para la administración de los recursos que el ordenador nos proporciona y los gestiona para un mejor rendimiento de la base de datos.

Una buena instalación y configuración de SQL Server, y sobre todo una buena administración de las herramientas que éste nos proporciona, logrará:

- Qué las consultas que se realicen mediante sentencias SQL obtengan un tiempo de respuesta óptimo.
- Qué la memoria y la CPU de la máquina estén aprovechadas al máximo.

Transact-SQL es el lenguaje que utiliza SQL Server para poder enviar peticiones tanto de consultas, inserciones, modificaciones, y de borrado a las tablas, así como otras peticiones que el usuario necesite sobre los datos. En definitiva, es un lenguaje que utiliza SQL Server para poder gestionar los datos que contienen las tablas.

El lenguaje estándar SQL (Structured Query Language) se emplea para los sistemas de bases de datos relacionales RDBMS (Relational Database Management System), es el estándar ANSI (American National Standards Institute). También es utilizado por otros sistemas como: Oracle, Access, Sybase, etc."[11]

"SQL Server 2008 es un elemento fundamental de la Plataforma de Datos de Microsoft, capaz de gestionar cualquier tipo de datos, en cualquier sitio y en cualquier momento. Le permite almacenar datos de documentos estructurados, semiestructurados o no estructurados como son las imágenes, música y archivos directamente dentro de la base de datos. SQL Server 2008 le ayuda a obtener más rendimiento de los datos, poniendo a su disposición una amplia gama de servicios integrados como son consultas, búsquedas, sincronizaciones, informes y análisis. Sus datos pueden almacenarse y recuperarse desde sus servidores más potentes del Data Center hasta los desktops y dispositivos móviles, permitiéndole tener un mayor control sobre la información sin importar dónde se almacena físicamente.

SQL Server 2008 le permite utilizar sus datos en aplicaciones a medida desarrolladas con Microsoft® .NET y Visual Studio y también desde su propia Arquitectura Orientada a Servicio (SOA) y los procesos empresariales empleando Microsoft® BizTalk® Server.

Además, las personas que gestionan la información pueden acceder directamente a los datos con las herramientas que utilizan habitualmente como Microsoft® Office 2007. SQL

11 http://www.formaselect.com/curso/experto-en-sql-server-2000/Introduccion-a-SQL-Server%202000.pdf

Server 2008 le ofrece una plataforma de datos, fiable, productiva e inteligente para cubrir todas sus necesidades."[12]

12 http://www.intercambiosvirtuales.org/software/microsoft-sql-server-2008-r2-enterprise-edition-dvd-espanol

5.2 MARCO CONCEPTUAL

AUDITORIA, revisión y evaluación de documentación física o lógica de una empresa o sociedad, realizada por un auditor.

Con frecuencias existen normativas que obligan a las empresas o compañías a realizar tipos de auditorías a los diferentes procesos ya sean de los sistemas de información o documentación contables etc.

RIESGO, Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Se mide en términos de una combinación de la probabilidad de que suceda un evento y sus consecuencias.

CONTROL, Cualquier acción tomada por la Gerencia para mejorar la probabilidad de que los objetivos establecidos sean alcanzados. Las diferentes empresas se han visto en la necesidad de imprentar controles en los sistemas de información y o otros procesos internos para su efectiva producción interna.

PROBABILIDAD, Es el número de veces que se da un evento, se define como el número de veces que una amenaza deja de serlo para convertirse en realidad, a lo largo de un determinado periodo de tiempo.

SEVERIDAD, Es la evaluación del efecto y consecuencia del riesgo. Generalmente, la exposición al riesgo se mide en aspectos económicos, imagen de las personas o empresas, disminución de capacidad de respuesta y competitividad, interrupción de operaciones, etc. Efecto que causa en la empresa la ocurrencia de un siniestro y que normalmente se ve reflejado en la suspensión de las actividades normales del negocio.

MODELO DE MADUREZ, Es un conjunto estructurado de elementos que describen el nivel de madurez de un ente en un aspecto determinado.

Establece un orden claro, discreto y absoluto, definiendo niveles o etapas de madurez. Establece de manera explícita la evolución de la organización en dicho aspecto

Me permite medirme (Autoanálisis). ¿Dónde estoy hoy? Me permite dónde debo estar. Me permite planear lo que debo lograr para llegar a donde quiero estar. Me permite gestionar mi crecimiento y evolución.

SISTEMAS, Conjunto de cosas que ordenadamente relacionados entre sí que contribuyen a un fin determinado. Los sistemas son distribuciones de varios procesos, que cumplen con una sola finalidad de compactar los resultados de una cadena de información estructural.

MALWARE, Son aquellos programas o partes de ellos que tienen un efecto malicioso en la seguridad del ordenador. Es el software malicioso o software potencialmente no deseado instalado sin el permiso de usuario adecuado. Malware es la abreviatura de "software malicioso". Es cualquier tipo de software no deseado que se instala sin el

consentimiento adecuado. Los virus, gusanos y caballos de Troya son ejemplos de software malicioso que se agrupan a menudo juntos.

SOFTWARE, Se conoce como software al equipamiento lógico o soporte lógico de un sistema informático, comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos, que son llamados hardware.

Los componentes lógicos incluyen, entre muchos otros, las aplicaciones informáticas; tales como el procesador de texto, que permite al usuario realizar todas las tareas concernientes a la edición de textos; el software de sistema, tal como el sistema operativo, que, básicamente, permite al resto de los programas funcionar adecuadamente, facilitando también la interacción entre los componentes físicos y el resto de las aplicaciones, y proporcionando una interfaz con el usuario.

La interacción entre el Software y el Hardware hace operativa la máquina, es decir, el Software envía instrucciones al Hardware haciendo posible su funcionamiento.

HARDWARE, El hardware de un ordenador lo componen todas las partes físicas y tangibles que componen todo el sistema que hace posible el funcionamiento del proceso de datos. Entre las partes más importantes que componen el hardware de un ordenador se encuentra el procesador o microprocesador, antiguamente conocido como CPU (Unidad Central de Procesamiento), que es el cerebro o corazón del sistema, por el cual pasan todos los datos, la placa base, o placa madre, que contiene todos los circuitos que interconectan los componentes del hardware.

6. DISEÑO METODOLÓGICO

6.1 TIPO DE ESTUDIO

En el presente trabajo se utilizó el tipo de investigación analítico –descriptivo, con el fin de analizar los riesgos existentes y describir los diferentes controles para minimizar los riesgos que se encuentran en el sistema de información médica MEDULA en el módulo de consulta externa, desarrollado por la empresa CompGenioss. Además se utilizaran conocimientos teóricos de los estándares denominados como "mejores prácticas" enfocado específicamente del marco de referencia COBIT para la administración del riesgo y el nivel de madurez de aplicativo.

6.2 MÉTODO DE ESTUDIO

La investigación desarrollada se enmarca en el área del conocimiento en auditoria de sistemas de información en el área de administración y control del riesgo orientado hacia el mejoramiento de la gestión empresarial para lograr una mayor productividad y competitividad

6.3 TÉCNICAS Y HERRAMIENTAS DE RECOLECCIÓN DE INFORMACIÓN

Como herramientas para la recolección de los datos en esta investigación se solicitaron la documentación pertinente a: Políticas de seguridad o procedimientos formales de la organización, manuales de usuarios y técnicos del aplicativo. La solicitud de esta documentación, fue el primer paso a realizar en una auditoria, a fin de obtener información relevante y adquirir una visión objetiva del proceso o sistema auditado.

Además se realizaron entrevistas como la técnica para conseguir informaciones necesarias que sirvan de aval para el buen desempeño del trabajo de investigación, se elaboró un listado de preguntas en el que se respondió SI o NO, por los entrevistados, específicamente es una lista de chequeo en el que permite al auditor tener claro lo que necesita saber, y por qué. Sus cuestionarios han sido vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, este documento permitió al auditor conversar y hacer preguntas normales, que en realidad aportaron para el cumplimiento de sus Cuestionarios

7. DELIMITACIÓN DEL PROYECTO

7.1 DELIMITACIÓN TEMPORAL

La delimitación temporal viene dada a partir de diciembre de 2011 y se tiene previsto que para el mes de julio de 2012 se logren los objetivos y alcance de este proyecto de manera satisfactoria.

Por lo anteriormente mencionado la delimitación temporal de este proyecto está enmarcada por un periodo de tiempo comprendido entre el mes de Diciembre de 2011 hasta el mes de Julio de 2012, con una temporalidad de aproximadamente 8 meses.

7.2 DELIMITACIÓN TÉCNICA

La delimitación técnica de este proyecto se encuentra definida por las principales herramientas tecnológicas que se utilizaron a lo largo del desarrollo del mismo:

- ✓ El sistema de información MEDULA es la herramienta principal para la realización de los objetivos y alcances especificados inicialmente.
- ✓ El motor de la base de datos en el cual se apoya MEDULA es SQL SERVER 2008.
- ✓ Management Studio Express 2008 como apoyo grafico del motor de la base de datos SQL SERVER 2008.
- ✓ El Aplicativo está diseñado para funcionar correctamente en sistemas operativos Microsoft Windows XP, Microsoft Windows Vista, Microsoft Windows 7.

7.3 DELIMITACIÓN FINANCIERA

Para la realización de este proyecto se generaron los siguientes gastos:

Concepto	Valor
Transporte Urbano	$ 180.000,00
Papelería	$ 150.000,00
Asesorías	$ 500.000,00
Gastos Varios	$ 70.000,00

Tabla 2. Presupuesto del proyecto

Total gastos empleados para la realización del proyecto: $ 900.000

8. CRONOGRAMA DE ACTIVIDADES

8.1 LISTADO DE ACTIVIDADES

Id		% completado	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
0	✓	**100%**	**AUDITORIA AL SISTEMA MEDULA**	**129 días**	**lun 23/01/12**	**vie 03/08/12**	
1	✓	**100%**	**PLANEACION DE LA AUDITORIA**	**28 días**	**lun 23/01/12**	**vie 02/03/12**	
2	✓	100%	Reunion con el Coordinador de COMPGENIOSS LTDA	1 día	lun 23/01/12	lun 23/01/12	
3	✓	100%	Establecer objetivos de la auditoria	9 días	mar 24/01/12	vie 03/02/12	2
4	✓	100%	Establecer el alcance de la auditoria	5 días	lun 06/02/12	vie 10/02/12	2
5	✓	100%	Definicion de requisitos para el desarrollo de la auditoria	5 días	lun 13/02/12	vie 17/02/12	2,3,4
6	✓	100%	Documentar el programa de trabajo	8 días	mié 22/02/12	vie 02/03/12	5
7	✓	**100%**	**EJECUCION DE LA AUDITORIA**	**95 días**	**lun 05/03/12**	**jue 26/07/12**	**1**
8	✓	100%	Reunion de apertura con la gerencia para confirmar el programa de auditoria	1 día	lun 05/03/12	lun 05/03/12	6
9	✓	100%	Aplicar correciones al programa de auditoria	4 días	mar 06/03/12	vie 09/03/12	8
10	✓	100%	Entrega de la carta de inicio	1 día	lun 12/03/12	lun 12/03/12	9
11	✓	100%	Conocer y entender el aplicativo	16 días	mar 13/03/12	mié 04/04/12	10
12	✓	100%	Supervision del Proyecto	1 día	lun 09/04/12	lun 09/04/12	11
13	✓	100%	Selección de Procesos y Objetivos de control Cobit 4.1	4 días	mar 10/04/12	vie 13/04/12	12
14	✓	100%	Realizar entrevistas en base a los procesos seleccionados	1 día	lun 16/04/12	lun 16/04/12	13
15	✓	100%	Alineacion de los Objetivos de control con ISO 27002 e Itil V3	3 días	mar 17/04/12	jue 19/04/12	14
16	✓	100%	Supervision del Proyecto	1 día	vie 20/04/12	vie 20/04/12	15
17	✓	100%	Elaboracion de Lista de chequeo	2 días	lun 23/04/12	mar 24/04/12	16
18	✓	100%	Visita para contestar la lista de chequeo	1 día	mié 25/04/12	mié 25/04/12	17
19	✓	100%	Analisis de la lista de chequeo	2 días	jue 26/04/12	vie 27/04/12	18
20	✓	100%	Supervision del Proyecto	1 día	lun 30/04/12	lun 30/04/12	19
21	✓	100%	Preparacion de pruebas	3 días	mié 02/05/12	vie 04/05/12	20
22	✓	100%	Ejecucion y analisis de las pruebas	5 días	lun 07/05/12	vie 11/05/12	21
23	✓	100%	Creacion del Set de pruebas	3 días	lun 14/05/12	mié 16/05/12	22
24	✓	100%	Supervision del Proyecto	1 día	jue 17/05/12	jue 17/05/12	23
25	✓	100%	Analisis de riesgo	10 días	vie 18/05/12	vie 01/06/12	24
26	✓	100%	Identificar escenarios de riesgos	2 días	lun 04/06/12	mar 05/06/12	25
27	✓	100%	Identificacion de los riesgos	3 días	mié 06/06/12	vie 08/06/12	26
28	✓	100%	Creacion de controles	3 días	mar 12/06/12	jue 14/06/12	27
29	✓	100%	Supervision del Proyecto	1 día	vie 15/06/12	vie 15/06/12	28
30	✓	100%	Creacion de mapa de riesgos	2 días	mar 19/06/12	mié 20/06/12	29
31	✓	100%	Supervision del Proyecto	1 día	jue 21/06/12	jue 21/06/12	30
32	✓	100%	Tomas de evidencias	4 días	vie 22/06/12	mié 27/06/12	31

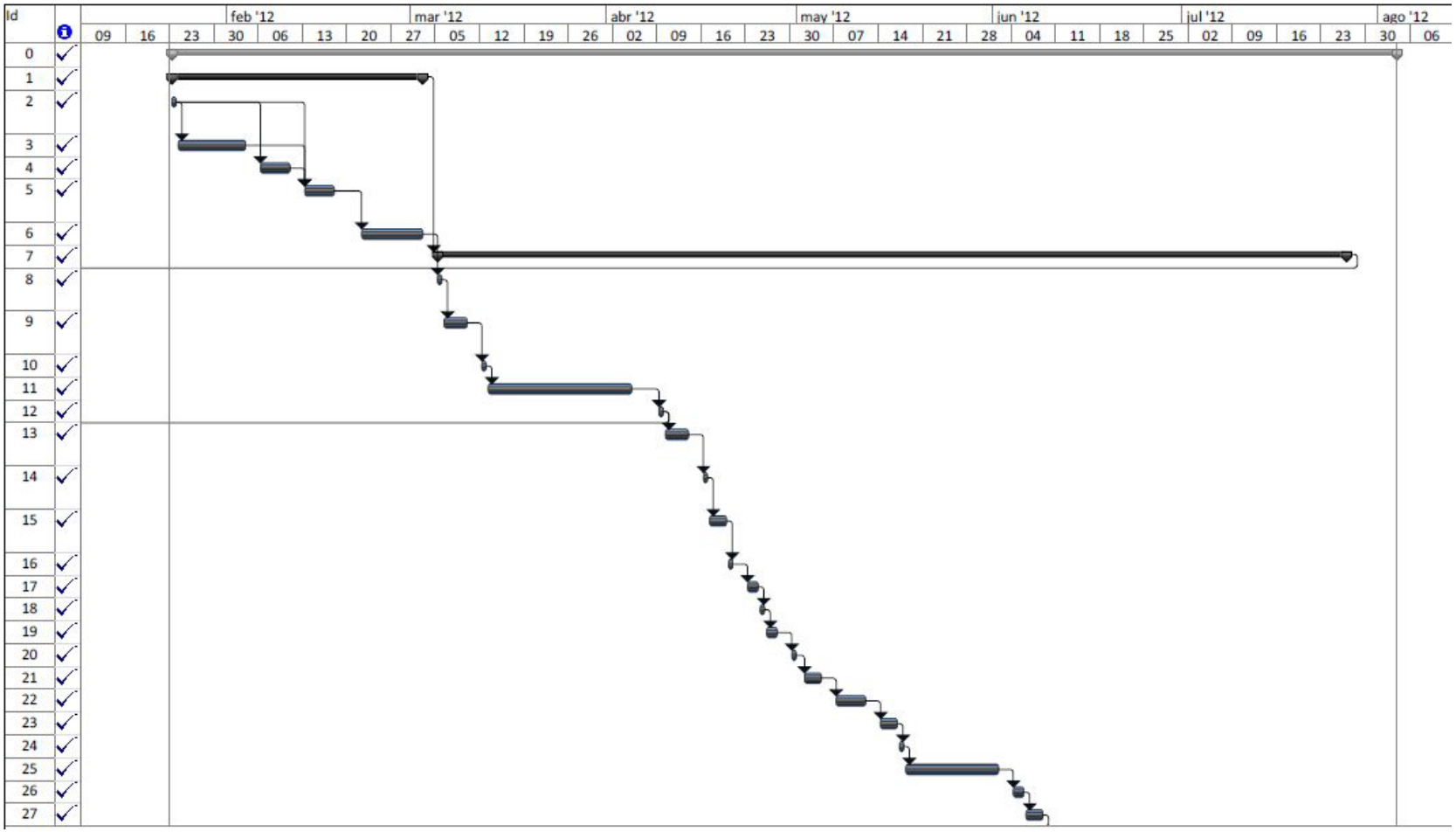
Id		% completado	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
34	✓	100%	Supervision del Proyecto	1 día	mar 03/07/12	mar 03/07/12	33
35	✓	100%	Identificar los hallazgos	4 días	mié 04/07/12	lun 09/07/12	34
36	✓	100%	Determinar Nivel de madurez de los procesos	4 días	mar 10/07/12	vie 13/07/12	35
37	✓	100%	Determinar nivel de madurez general del aplicativo	3 días	lun 16/07/12	mié 18/07/12	36
38	✓	100%	Supervision del proyecto	1 día	jue 19/07/12	jue 19/07/12	37
39	✓	100%	Recomendaciones y sugerencias	3 días	lun 23/07/12	mié 25/07/12	38
40	✓	100%	Supervision del Proyecto	1 día	jue 26/07/12	jue 26/07/12	39
41	✓	**100%**	**INFORMES DE AUDITORIA**	**77 días**	**mar 10/04/12**	**jue 02/08/12**	**7**
42	✓	100%	Creacion Informe Detallado	71 días	mar 10/04/12	mié 25/07/12	12
43	✓	100%	Creacion Informe Ejecutivo	4 días	vie 27/07/12	mié 01/08/12	40
44	✓	100%	Presentacion de los informes	1 día	jue 02/08/12	jue 02/08/12	42,43
45	✓	**100%**	**PAPELES DE TRABAJO**	**120 días**	**vie 03/02/12**	**vie 03/08/12**	**41**
46	✓	100%	Documentar Papeles de trabajo	118 días	vie 03/02/12	mié 01/08/12	
47	✓	100%	Entrega de papeles de trabajo	1 día	vie 03/08/12	vie 03/08/12	46,44

Figura 1. Lista de actividades

8.2 LINEA DE TIEMPO

Figura 2. Línea de Tiempo

8.3 DIAGRAMA DE GANTT



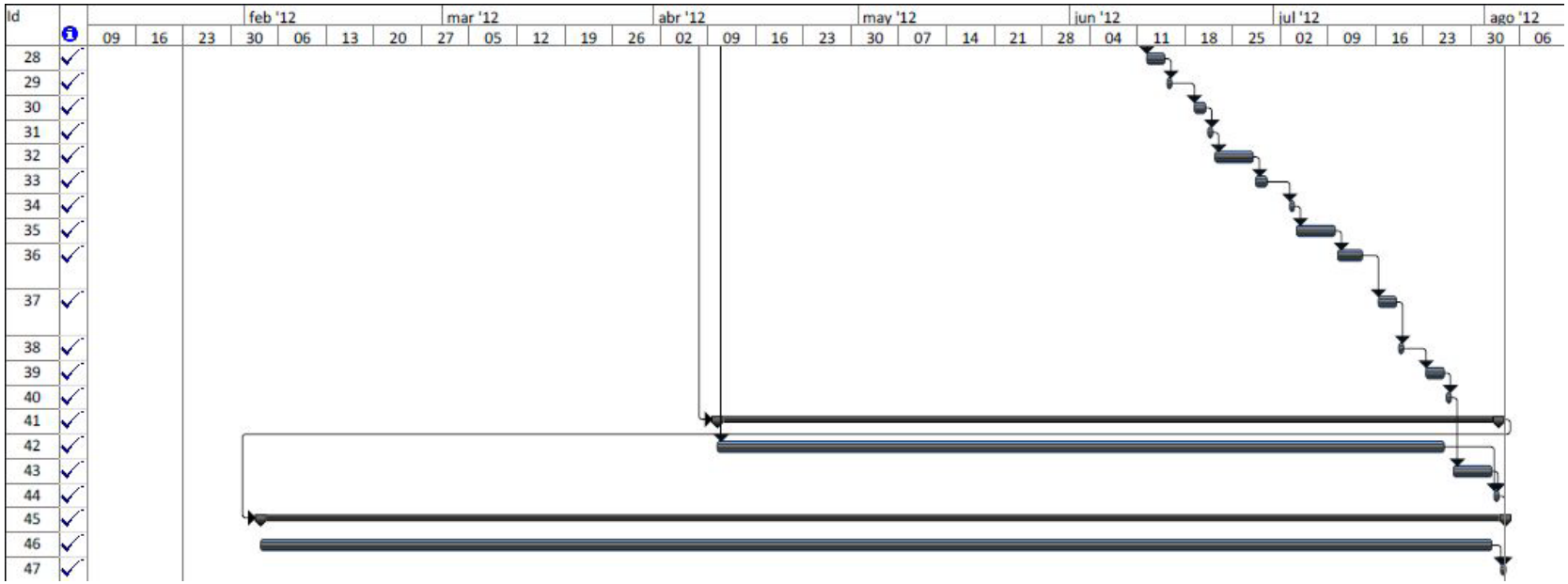


Figura 3. Diagrama de Gantt

9. CONFORMACIÓN Y TRAYECTORIA DE LOS RESPONSABLES

ESTA AUDITORIA FUE REALIZADA POR:

ALCIDES DE JESÚS GIOVANNETTI CAHUANA

Ingeniero de sistemas, de la Corporación Universitaria de la Costa CUC y Aspirante a especialista de auditoría de sistemas de información en la misma institución educativa.

Correo: alcidesgiovannetti@hotmail.com

Celular: 310 712 60 75

IRLETH KARINE FONSECA ZAMBRANO

Ingeniera de sistemas, de la Corporación Universitaria de la Costa CUC y Aspirante a especialista de auditoría de sistemas de información en la misma institución educativa.

Correo: irle0127@hotmail.com

Celular: 300 556 07 68

JOSÉ LUIS REDONDO AGUILAR

Ingeniero de sistemas, de la Corporación Universitaria de la Costa CUC y Aspirante a especialista de auditoría de sistemas de información en la misma institución educativa.

Correo: ing.joseluis.ra@hotmail.com>

Celular: 301 721 72 04

Los cuales se encuentran realizando una Auditoria Al Sistema De Información “MEDULA” De La Empresa CompGenioss LTDA. Aplicando Lineamientos de los estándares

denominados como “mejores prácticas” enfocado específicamente al marco de referencia COBIT, para identificar posibles riesgos y proponer alternativas de solución a la empresa

Para lograr un desarrollo completo y efectivo de la auditoria al aplicativo MEDULA, es necesario cumplir una serie de pasos o actividades, en donde cada una de estas, arroja resultados, que al final serán las pruebas del correcto desarrollo de la auditoria, en este caso, se efectuaron las siguientes actividades:

- **Plan de auditoría:** En él se identificó el alcance, el objetivo y la metodología que se utilizó durante el desarrollo de la auditoria.

- **Carta de inicio:** En este documento, se dio a conocer a CompGenioss LTDA. de manera formal el inicio de la auditoria en su organización. En él se describe el objetivo, alcance y los requerimientos para realizar la auditoria.

- **Lista de chequeo:** En este documento se elaboró un listado de preguntas donde el entrevistado respondió SI o No, además de algunas observaciones, esta lista de chequeo estuvo dirigida a todo el personal de CompGenioss LTDA. el cual permite al auditor tener claro puntos importantes al momento de realizar la auditoria.

- **Entrevistas:** En este documento se realizaron entrevistas al gerente general y al gerente de operación tecnológica de CompGenioss LTDA., teniendo como base los procesos COBIT seleccionados.

- **Informe detallado:** En este informe se muestran todos los resultados obtenidos durante el desarrollo de la auditoria.

- **Set de pruebas:** En este documento se describe las pruebas desarrolladas en el módulo de consulta externa del sistema de información MEDULA, generando un reporte general, el cual posee todos y cada uno de los hallazgos encontrados.

- **Alineación de Marcos de Referencia:** En él se hace una relación de los objetivos de control de COBIT 4.1 seleccionados para el desarrollo de la auditoria CON ITIL V3 E ISO 27002.

- **Nivel de madurez para cada proceso COBIT 4.1:** En este documento se describe el nivel de madurez de los procesos seleccionados mediante el esquema definido por el marco de referencia COBIT 4.1.

- **Informe ejecutivo:** En este informe se realiza un breve análisis de los aspectos más importantes de la auditoría realizada al módulo de consulta externa del sistema de información MEDULA.

10. INFORMES DE LA AUDITORIA

10.1 INFORME EJECUTIVO

UNIVERSIDAD DE LA COSTA

INFORME EJECUTIVO

AUDITORIA AL MODULO DE CONSULTA EXTERNA DEL SISTEMA DE INFORMACIÓN MEDULA DE LA EMPRESA COMPGENIOSS LTDA.

Ingeniero: Bladimir Cahuana

Julio de 2012

Barranquilla, Agosto 6 de 2012

Ing.

BLADIMIR CAHUANA

Gerencia CompGenioss LTDA.

E. S. M.

Ref: Informe con los resultados de la Auditoría al Sistema de Información Medula, en el módulo de consulta externa

Cordial saludo,

Nos complace presentar a su consideración el informe con los resultados de la Auditoria al módulo de consulta externa del Sistema de Información Medula.

10.1.1 OBJETIVOS Y ALCANCE DE LA AUDITORIA

La auditoría tuvo como objetivo realizar una auditoría al sistema de información Medula en el módulo de consulta externa para identificar posibles riesgos y proponer alternativas de solución a la empresa, realizar un análisis para determinar los riesgos que pueden presentarse e impedir el correcto funcionamiento del aplicativo Medula o comprometer la seguridad de la información, verificar los controles existentes del módulo de consulta externa en el Software y complementarlos, determinar el nivel de madurez del aplicativo

utilizando como apoyo el marco de referencia COBIT, e incluyó en Verificar la seguridad, la integridad, y el procesamiento de datos del aplicativo Medula

En nuestra revisión evaluamos y verificamos los controles en los siguientes procesos de la aplicación:

- ✓ Acceso y seguridad
- ✓ Base de datos
- ✓ Documentación del Sistema
- ✓ Ergonomía del aplicativo
- ✓ Pruebas del software
- ✓ Portabilidad del Software
- ✓ Trazabilidad del aplicativo
- ✓ Copias de Respaldos (Backup)
- ✓ Funcionalidad del aplicativo
- ✓ Control de Cambios

10.1.2 METODOLOGIA EMPLEADA

La Auditoría se desarrolló de acuerdo con las normas, lineamientos y estándares denominados “Mejores Prácticas”.

Para satisfacer los objetivos de la auditoría se desarrollaron los siguientes pasos y procedimientos:

a. Se efectuaron entrevistas con el Gerente General Vladimir Cahuana, y el Gerente de operación Tecnológica Carlos Novoa, con el propósito de obtener información del ambiente técnico, operativo y administrativo del Sistema de Información Medula.

b. Siguiendo las recomendaciones de los estándares denominados “Mejores Prácticas” ,COBIT 4.1 (Control Objetives for Information an Related Technolgy), ITIL V3 (Information Technology Infrastructure Library), e ISO/IEC 27002, se realizó un ejercicio de análisis de riesgos asociados con el Sistema de Información Medula.

c. Con base en los resultados del análisis de riesgos, se inició el proceso de “auditoría orientada al riesgo”. Este proceso consistió en a) Identificar los posibles riesgos y escenarios de riesgo. b) Identificar y evaluar los controles existentes. c) Diseñar y ejecutar las pruebas de auditoría d) Toma de evidencias y e) Elaboración y presentación del informe con los resultados de la Auditoría.

10.1.3 LIMITACIONES PARA EL DESARROLLO DE LA AUDITORIA

No se evaluó ni se verificó la documentación del sistema de información Medula debido a la inexistencia de la documentación técnica del sistema.

10.1.4 HALLAZGOS

A. CompGenioss no tiene identificados los riesgos y su ocurrencia, en ninguna etapa del proyecto se realizó una valoración de riesgos.
B. No se tiene implementación de un plan de acción de riesgos.
C. CompGenioss no cuenta con políticas definidas de cómo se debe realizar el emprendimiento de nuevos proyectos.
D. Algunos de los proyectos no se logran entregar en el tiempo estipulado en el cronograma
E. En algunas ocasiones los costos han sobrepasado el presupuesto establecido para el desarrollo del proyecto.
F. No se tienen identificados los riesgos que se pueden presentar en el desarrollo del proyecto
G. Cuando se realizan cambio en el cronograma y en el presupuesto estos se están informando al encargado y adicionalmente se les está haciendo su respectiva documentación
H. CompGenioss no ha verificado que MEDULA cumpla con las legislaciones y regulaciones establecidas por la ley lo cual puede ser causal de sanciones y penalizaciones.
I. El aplicativo no tiene la posibilidad de ser auditado sin embargo la base de datos que está realizada en SQL SERVER 2008 si cuenta con esta fortaleza.
J. No se ha verificado la seguridad del aplicativo.
K. Se les está comentando a los posibles clientes la importancia del cambio de tecnología.
L. El aplicativo MEDULA no cuenta con manuales de usuarios para el uso del sistema y de igual forma no cuenta con los manuales de operaciones y soporte, para la configuración y mantenimiento del aplicativo o algún documento formal que pueda servir de ayuda para el cliente.

M. CompGenioss no cuenta con procesos y políticas definidas para la adquisición de recursos de TI, solo se realiza una investigación de mercado y se selecciona la que mejor se ajuste a las necesidades de la empresa basándose sobre todo en la marca y en el precio.

N. No se está documentando el registro de los recursos de TI que adquiere la organización.

O. Cuando se adquieren nuevos recursos de TI no se les realiza capacitación a los empleados únicamente les comentan sobre la tecnología adquirida.

P. Para la adquisición de recursos de TI se cuenta con la aprobación del Gerente General el señor Bladimir Cahuana.

Q. CompGenioss no cuenta como un procedimiento formal ni con una autorización previa para realizar cambios en el aplicativo

R. No se tiene documentado el manual de usuario, solo se le hacen las pruebas para probar pero no se documenta nada

S. No se establece un plan de pruebas ni ambiente de prueba; Las pruebas las realiza el desarrollador según su criterio en el momento en el que él las indique

T. Algunas veces se evalúan y se aprueban los resultados de las pruebas por parte de la gerencia de la compañía

U. Cuando se realizan los cambios se le hace una revisión posterior a la implantación

V. Las cuentas de los usuarios del aplicativo, tienen roles y perfiles similares, lo cual no permite identificar cual es el usuario administrador del aplicativo y cual es un usuario con privilegios restringidos.

10.1.5 MATRIZ DE RIESGO POR PROCESOS COBIT

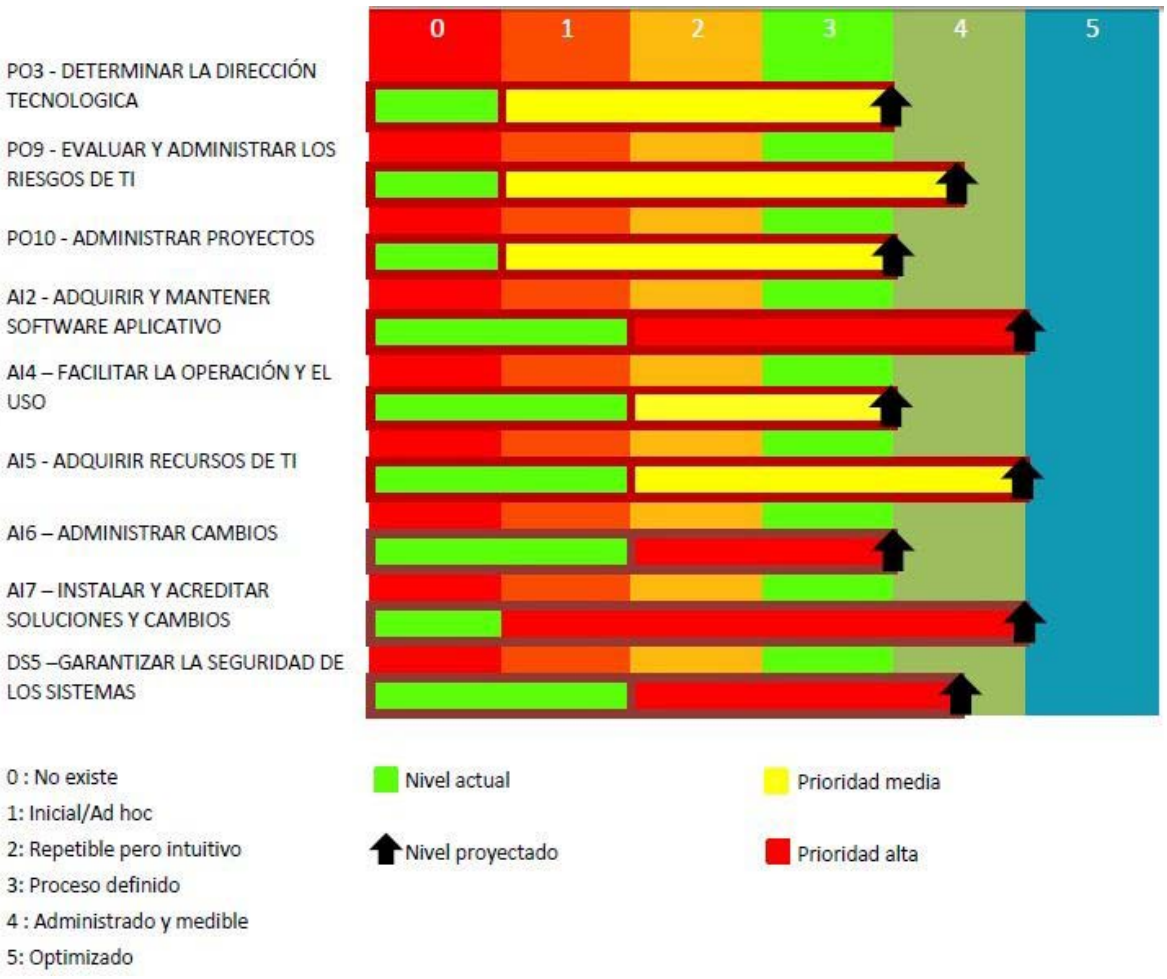


Figura 4. Matriz de Riesgo por Proceso COBIT

10.1.6 RESULTADOS DE LA AUDITORIA

10.1.6.1 OPINION DE LA AUDITORIA

- No se está realizando una debida gestión y documentación para la administración de los riesgos de TI lo cual imposibilita una adecuada respuesta en caso tal de que un riesgo logre materializarse siendo esto causante de pérdidas de dinero, insatisfacción del cliente con los productos adquiridos y perdida de la imagen comercial de la empresa. Por ende se CompGenioss debe ser consciente de la importancia de realizar una adecuada valoración de riesgos de TI antes de emprender el desarrollo de un nuevo aplicativo.

- Es indispensable la creación de una política o marco de trabajo que entre a regir el cómo y el porqué de la realización de un nueva proyecto de TI, esto debe realizarse con el fin de garantizar excelente resultados y la calidad del mismo; se debe tener presente los riesgos, recursos, pruebas, entregables y costos para el desarrollo con éxito de los proyectos de TI.

- CompGenioss en estos momentos está realizando una inadecuada gestión para la adquisición de recursos de TI ya que no cuenta con una política definida para dicha gestión simplemente se apoyan en el reconocimiento de la marca o el precio del producto adicionalmente no se están realizando las capacitaciones pertinentes para las tecnologías adquiridas, sin embrago para la adquisición de tecnología se cuenta con la autorización previa del gerente general.

- La instalación y acreditación de soluciones y Cambios en la organización es aceptable, debido a que las soluciones se identifican de manera informal con base en la experiencia de los desarrolladores, ellos son los que realizan las pruebas en el momento en el que él las indique ya que no existe un procedimiento formal a seguir dentro de la compañía. Se usan enfoques no estructurados para definir

los requerimientos e identificar las soluciones tecnológicas y cambios. En ocasiones la gerencia reconoce la necesidad de verificar que las soluciones se ajustan para el propósito deseado.

- CompGenioss se encuentra incumpliendo, uno de los requerimientos más importantes al momento de realizar y entregar un aplicativo, y es que no está transmitiendo al cliente la información necesaria para que este opere de forma segura y ágil el nuevo producto adquirido, ya sea por medio de manuales, documentos formales o capacitaciones, lo cual propiciara a futuro inmediato fallas y errores en el aplicativo, debido al desconocimiento del funcionamiento y configuración del nuevo sistema.

- En CompGenioss la administración de cambios en el aplicativo MEDULA es aceptable, debido a que no existe un proceso de administración de cambio informal, no existe autorización previa para realizar cambios, no se tiene conciencia de que el cambio puede causar una interrupción para TI y las operaciones de negocio, no se cuenta con procedimientos que sean utilizados para manejar todos los cambios de forma eficiente y rápida.

- En estos momentos el aplicativo MEDULA, se encuentra con una falla grave de seguridad, a nivel de acceso, debido a que no se tiene establecido de forma correcta los permisos y privilegios de todos los usuarios que manejan el sistema, lo que genera riesgo en el manejo, integridad y seguridad de la información. Esta falla debería ser solucionada lo antes posible, puesto que la clave de un buen sistema es la seguridad y el aplicativo MEDULA, tiene muchas deficiencias en esta área.

10.1.6.2 PRINCIPALES RECOMENDACIONES Y PUNTOS MEJORABLES

10.1.6.2.1 CONTROLES INTERNOS Y PROCEDIMIENTOS

A. Realizar una matriz de roles y perfiles, para segregar de forma adecuada y segura los permisos y privilegios que tienen los usuarios en el sistema.
B. Contar con un debido proceso, para la adecuada definición de roles y perfiles de los usuarios del sistema y de igual forma registrar todos estos procedimientos en dicha matriz.
C. Verificar que los software desarrollados por CompGenioss entre ellos MEDULA estén cumpliendo y cumplan con las legislaciones y regulaciones establecidas por la ley con el fin de evitar multas y sanciones.
D. Se debe verificar la seguridad de los productos tales como controles de accesos, cambio de contraseñas, longitud de las contraseñas, fortaleza de las contraseñas, etc.
E. La creación de manuales de usuarios para el aplicativo MEDULA con el fin de que el personal actual y futuro tenga una base de ayuda y guía, al momento de solucionar un inconveniente en algún proceso de la aplicación, además de ayudar en la realización de las tareas diarias del usuario.
F. La creación de los manuales de operaciones y soporte del aplicativo MEDULA, para que se puedan realizar de forma correcta y segura todas las instalaciones, configuraciones y mantenimientos necesarios.
G. Complementar la realización y entrega de los manuales, con capacitaciones periódicas, sobre el uso efectivo de todos los recursos de la herramienta, tanto a nivel de usuario final como a nivel de operaciones y soporte.

H. Se debe crear políticas para la adquisición de recursos de TI en las cuales se documente y se resalte una descripción detallada de los recursos adquiridos tal como la fecha de adquisición, marca, precio, proveedores, competencia en el mercado.

I. Se debe de realizar una documentación sobre los recursos de TI adquiridos así como también los nuevos adquirir con el objetivo de llevar un control exhaustivo sobre estos activos que son sumamente importante para la organización.

J. Al momento de adquirir una nueva tecnológica se debe capacitar a los empleados sobre el producto adquirido brindándole la oportunidad de entender sus funcionamiento, funcionalidad así como de resolver sus dudas e inquietudes.

K. Establecer políticas y procedimientos formales para la administración de cambios en el aplicativo

L. Establecer un proceso formal para autorizar los cambios de emergencia que no sigan el proceso de cambio establecido

M. Establecer un plan y un ambiente de prueba, y que este sea aprobado por las partes relevantes de la organización.

N. Realizar revisiones post implementación a los cambios realizados al aplicativo.

10.1.6.2.2 ORGANIZACION E INFORMACION

A. Realizar un plan de acción de riesgos que pueden presentarse antes, durante y después del desarrollo del proyecto.

B. Realizar una adecuada valoración de riesgos la cual valide su probabilidad de ocurrencia y el impacto.

C. Llevar al corriente la documentación de eventos y sucesos que se presenten en el ciclo de vida de los proyectos.

D. La realización de políticas que sirvan como guías para el desarrollo de nuevos proyectos.
E. Tomar medidas adecuadas para el manejo de los recursos entre ellos dinero, personal, equipos de cómputo.
F. Realizar una adecuada gestión de riesgos del proyecto para tener documentados las posibilidades de ocurrencia y el impacto con el objetivo de mitigar y prevenir la ocurrencia de los mismos.
G. Documentar el manual de usuarios del aplicativo y actualizarlo cada vez que se realice un cambio en la aplicación.
H. Se debe asegurar que el dueño del proceso de negocio y los interesados de TI evalúen los resultados de los procesos de pruebas.

Se hace entrega de este informe el día -- de Agosto de 2012 a los señores Bladimir Cahuana, Gerente General de CompGenioss LTDA. y Carlos Novoa, Gerente de Operación Tecnológica

Cordialmente,

Alcides Giovannetti Cahuana
Auditor de Sistemas
CC. 1.042.349.216 S/grande

Irleth Fonseca Zambrano
Auditora de Sistemas
CC. 1.043.001.010 S/larga

José Redondo Aguilar
Auditor de Sistemas
CC. 1.129.513.615 B/quilla

10.2 INFORME DETALLADO

UNIVERSIDAD DE LA COSTA

INFORME DETALLADO

AUDITORIA AL MODULO DE CONSULTA EXTERNA DEL SISTEMA DE INFORMACIÓN MEDULA DE LA EMPRESA COMPGENIOSS LTDA.

Ingeniero: Bladimir Cahuana

Julio de 2012

INTRODUCCION

COMPGENIOSS LTDA. es una organización que tiene como actividad comercial el desarrollo de software a la medida, consultoría, asesorías y sistematización en general, tiene 14 años de servicio y representa más de 10.000 productos tecnológicos instalados, mas de 14.000 hrs en proyectos de investigación y desarrollo tecnológico, mas de 11.000 hrs en proyectos de desarrollo empresarial, más de 15.000 metros en conexiones de comunicación y más de 50 aplicaciones de software instaladas.

COMPGENIOSS LTDA. optó por desarrollar un nuevo software para la gestión hospitalaria llamado MEDULA el cual es un sistema de información para las instituciones prestadora de salud (IPS) en todos sus niveles de atención y complejidad que involucra el manejo integral de la gestión administrativa y asistencial. MEDULA es un Software Integrado, diseñando bajo plataforma Cliente Servidor y está desarrollado para operar en ambiente Windows, de igual forma la gestión asistencial es soportada por una serie de módulos tales como: Urgencia, Hospitalización, Consulta externa, Historia clínica, Enfermería, Estadística y Facturación.

El aplicativo MEDULA en estos momentos se encuentra en proceso de prueba en el E.S.E Hospital de San Onofre y se planea implementar este software en otras entidades.

Se realizó la auditoría al Aplicativo MEDULA en el modula de CONSULTA EXTERNA, utilizando como Marco de Referencia COBIT 4.1 el cual se complementó con ISO 27002, ITIL V3 e ISO 3100, con el propósito de identificar las debilidades y fortalezas soportadas en estas buenas prácticas. Se identificaron los Riesgos relacionados con el Sistema soportados en la norma ISO 31000. El propósito principal es emitir recomendaciones que

pueden brindar a la gerencia la creación de estrategias y la identificación de controles que permitan transformar dichas debilidades en fortalezas y las amenazas en oportunidades.

10.2.1 DESCRIPCION TECNICA

10.2.1.1 ENTORNO AUDITABLE

MISIÓN

COMPGENIOSS LTDA, desea brindar todo el conocimiento y amplia experiencia a las empresas, para ayudar al logro de sus objetivos con el mayor grado de seguridad, aplicando novedosas estrategias y tecnologías, para el correcto desarrollo de las mismas.

VISIÓN

Ser una empresa líder en el mercado Colombiano, en las áreas de consultoría en sistemas y tecnología, orientando todos nuestros esfuerzos en el éxito de nuestros clientes, brindando servicios de gestión empresarial y soluciones de sistemas de la más alta calidad.

10.2.1.2 ORGANIGRAMA GENERAL COMPGENIOSS LTDA.

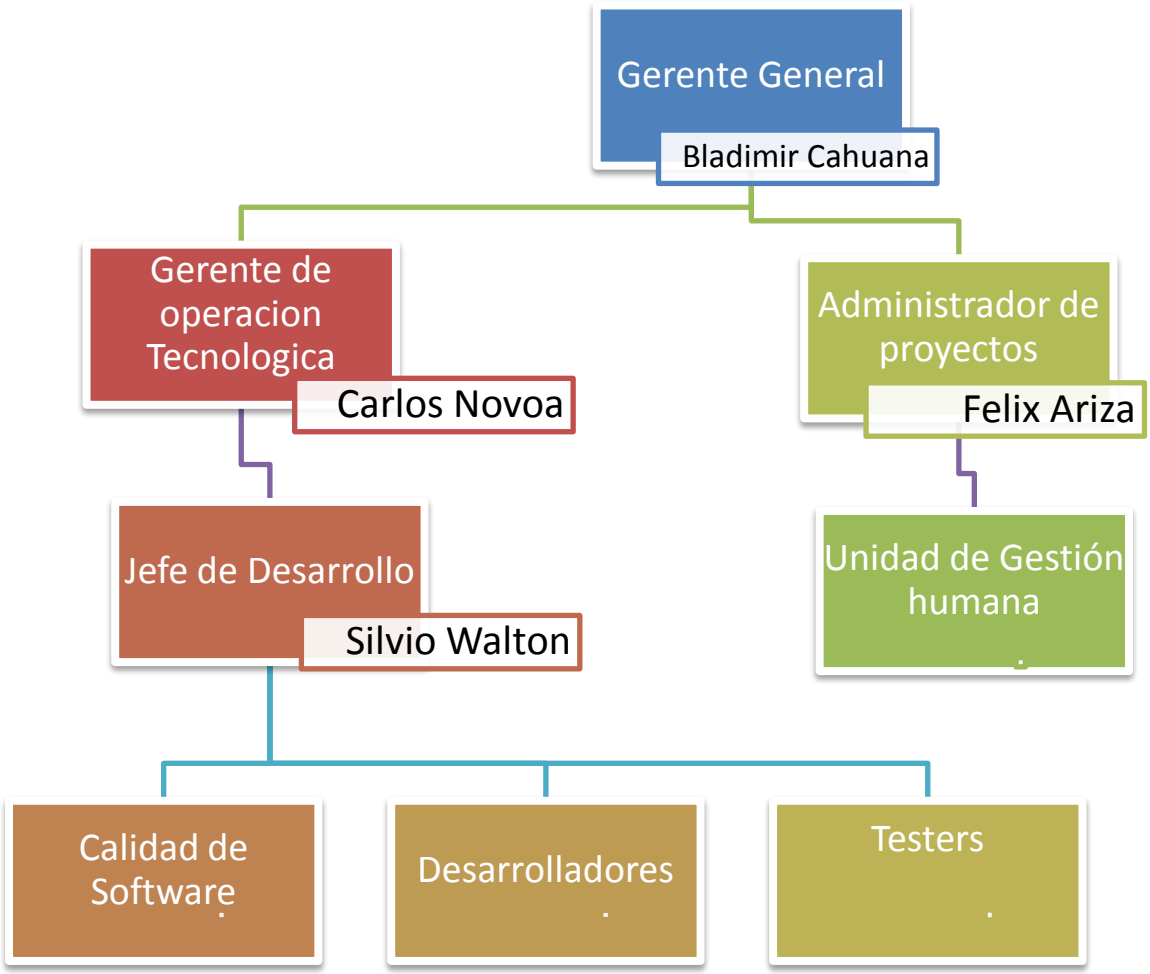


Figura 5. Organigrama general

10.2.2 ANÁLISIS DE RIESGOS

Debido a que la empresa COMPGENIOSS LTDA. No contaba con una identificación de los riesgos que puedan afectar e impactar de manera negativa su nuevo software MEDULA se realizó una auditoria en la cual se identificaron, riesgos con sus respectivos escenarios y los controles, todo esto apoyado en los estándares denominados como mejores prácticas, principalmente COBIT 4.1 el cual fue complementado con ITIL V3, ISO 27002, ISO 3100.

10.2.2.1 ESCENARIOS DE RIESGOS

Como parte fundamental del análisis de riesgo es necesario establecer los escenarios de riesgos en donde se permite identificar las posibles amenazas y vulnerabilidades a los que son expuestos el software MEDULA

Los escenarios de riesgos detectados en el proceso de auditoría desarrollada al aplicativo MEDULA, específicamente en el módulo de Consulta Externa, son:

1. Acceso y seguridad
2. Base de datos
3. Documentación
4. Ergonomía
5. Pruebas del Software
6. Portabilidad
7. Trazabilidad del aplicativo

8. Copias de Respaldo (Backup)
9. Funcionalidad
10. Control de cambios

10.2.2.2 RIESGOS IDENTIFICADOS

Teniendo en cuenta que se considera como riesgo cualquier circunstancia, evento, amenaza, acto u omisión, que pueda en un momento dado impedir el logro de los objetivos estratégicos formulados por la alta dirección, o la exitosa implementación de las estrategias, se desarrolló una auditoria en la cual se identificaron los posibles riesgos los cuales son:

1. Inadecuados o ausencia de controles de Seguridad
2. Inadecuados o Inexistentes controles de nivel de acceso al sistema
3. Pérdida de información debido que el sistema presente inconsistencia en la base de datos
4. Inexistencia o desactualización de documentación del Sistema
5. Interfaz de usuario compleja
6. Ausencia o Inadecuada realización de Pruebas de Software
7. Inadecuada portabilidad del Sistema
8. Ausencia de Pistas de Auditoria
9. Ausencia de copias de respaldo
10. Perdidas de información registrada en el sistema e inconsistencia en el funcionamiento de los diferentes módulos del aplicativo.
11. Inadecuado o inexistencia de gestión de cambios del aplicativo

10.2.2.3 CONTROLES

Los controles son las acciones que se toman en busca de reducir la probabilidad y el impacto de ocurrencia de un riesgo que pueda impactar el logro de los objetivos de un negocio o proceso, teniendo en cuenta lo anterior y luego de desarrollar la auditoria se establecieron los siguientes controles:

1. Parametrizar correctamente los campos del aplicativo
2. Implementar Políticas para la Protección y seguridad de los Datos
3. Definir e implementar políticas de roles y perfiles para el acceso a la base de datos.
4. Validar los controles de acceso al sistema.
5. Implementar políticas y procedimientos para la administración de la BD
6. Documentar procedimientos y cambios que se realicen en la base de datos
7. Adecuada integridad y consistencia de la base de datos
8. Actualizar periódicamente la documentación del sistema (Incluye manuales técnicos- usuario - instalación)
9. Documentar los requerimientos funcionales del sistema.
10. Documentar procedimientos y cambios que se realicen en la base de datos
11. Capacitar a los usuarios finales sobre el correcto uso y administración del aplicativo.
12. Apropiado desarrollo del diseño de interfaz de usuario
13. Documentar, Ejecutar y aceptar pruebas del aplicativo por parte del usuario

14. Identificar la plataforma en donde se va a implementar el aplicativo.
15. Adecuado desarrollo y diseño del aplicativo con facilidad de ser altamente auditable
16. Definir e implementar Políticas de Respaldo
17. Establecer un sitio alterno para salvaguardar la información
18. Realizar copias de respaldo (Backup)
19. Implementar bitácora de fallas para identificar problemas que presente el aplicativo.
20. Definir e implementar instrucciones, para evitar la entrada no autorizada de cambios en el sistema.
21. Establecer procedimientos de nuevos cambios en el aplicativo.
22. Documentar registros sobre los cambios realizados al aplicativo.

10.2.2.4 RIESGOS, CONTROLES Y ESCENARIOS

Escenarios	#	Riesgo	#	Control
Acceso y seguridad	1	Inadecuada definición o ausencia de controles de Seguridad	1	Parametrizar correctamente los campos del aplicativo
			2	Implementar Políticas para la Protección y seguridad de los Datos
	2	Inadecuado definición o Inexistente controles de nivel de acceso al sistema	3	Definir e implementar políticas de roles y perfiles para el acceso a la base de datos.
			4	Validar los controles de acceso al sistema.
Base de datos	3	Pérdida de información debido que el sistema presente inconsistencia en la base de datos	5	Implementar políticas y procedimientos para la administración de la BD
			6	Documentar procedimientos y cambios que se realicen en la base de datos
			7	Adecuada integridad y consistencia de la base de datos
Documentación	4	Inexistencia o desactualización de documentación del Sistema	8	Actualizar periódicamente la documentación del sistema (Incluye manuales técnicos- usuario - instalación)
			9	Documentar los requerimientos funcionales del sistema.
			10	Documentar procedimientos y cambios que se realicen en la base de datos
Ergonomía	5	Interfaz de usuario compleja	11	Capacitar a los usuarios finales sobre el correcto uso y administración del aplicativo.
			12	Apropiado desarrollo del diseño de interfaz de usuario

Pruebas del software	6	Ausencia o Inadecuada realización de Pruebas de Software	13	Documentar, Ejecutar y aceptar pruebas del aplicativo por parte del usuario
Portabilidad	7	Inadecuada portabilidad del Sistema	14	Identificar la plataforma en donde se va a implementar el aplicativo.
Trazabilidad del Sistema	8	Ausencia de Pistas de Auditoria	15	Adecuado desarrollo y diseño del aplicativo con facilidad de ser altamente auditable
Copias de Respaldos (Backup)	9	Ausencia o inadecuada definición de copias de respaldo	16	Definir e implementar Políticas de Respaldo
			17	Establecer un sitio alterno para salvaguardar la información
			18	Realizar copias de respaldo (Backup)
Funcionalidad	10	Inconsistencia en el funcionamiento de los diferentes módulos del aplicativo.	19	Implementar bitácora de fallas para identificar problemas que presente el aplicativo.
Control de Cambios	11	Inadecuado o inexistencia de gestión de cambios del aplicativo	20	Definir e implementar instrucciones, para evitar la entrada no autorizada de cambios en el sistema.
			21	Establecer procedimientos de nuevos cambios en el aplicativo.
			22	Documentar registros sobre los cambios realizados al aplicativo.

Tabla 3. Escenarios Vs Riesgos Vs Controles

10.2.2.5 MAPA DE RIESGOS

10.2.2.5.1 VALORACIÓN DEL NIVEL DE RIESGO

Probabilidad	Impacto	Nivel de riesgo
Casi Certeza	Catastrófico	Extremo
Casi Certeza	Mayor	Extremo
Casi Certeza	Moderado	Extremo
Casi Certeza	Menor	Alto
Casi Certeza	Insignificante	Alto
Probable	Catastrófico	Extremo
Probable	Mayor	Extremo
Probable	Moderado	Alto
Probable	Menor	Alto
Probable	Insignificante	Moderado
Posible	Catastrófico	Extremo
Posible	Mayor	Extremo
Posible	Moderado	Alto
Posible	Menor	Moderado
Posible	Insignificante	Bajo
Improbable	Catastrófico	Extremo
Improbable	Mayor	Alto
Improbable	Moderado	Moderado
Improbable	Menor	Bajo
Improbable	Insignificante	Bajo
Raro	Catastrófico	Alto
Raro	Mayor	Alto
Raro	Moderado	Moderado
Raro	Menor	Bajo
Raro	Insignificante	Bajo

Tabla 4. Valoración del nivel de riesgo

10.2.2.5.2 DEFINICION DE LA VALORACION DE LOS RIESGOS SEGUN SU PROBABILIDAD DE OCURRENCIA

Casi Certeza: Cuando se tiene la completa seguridad de que el evento no deseado va a ocurrir en cualquier momento.

Probable: Cuando el sistema presenta demasiadas debilidades y falencias que puedan ser causantes para la materialización de los riesgos.

Posible: Cuando el sistema presenta vulnerabilidades que pueden comprometer la estabilidad del mismo pero la materialización del riesgo depende de factores externos tal como personas, malware, otros.

Improbable: Cuando existen pocas vulnerabilidades y debilidades causantes de que los riesgos se materialicen.

Raro: es cuando la ocurrencia del riesgo es considerada prácticamente imposible de que suceda debe ser provocada por múltiples errores humanos así como entes externos al sistema.

10.2.2.5.3 DEFINICION DE LA VALORACION DE LOS RIESGOS SEGUN SU IMPACTO

Catastrófico: Un riesgo es considerado catastrófico cuando compromete la continuidad del negocio, representa grandes cantidades de pérdidas de activos entre los cuales destacan el dinero y la información.

Mayor: Un riesgo es considerado mayor cuando está comprometiendo la seguridad, confidencialidad y disponibilidad de la información o es causante de pérdidas significativas de activos.

Moderado: Un riesgo es considerado moderado cuando genera pérdidas mínimas de los activos de la compañía, además es causante de paralización de procesos y generador de reprocesaos de manera reiterativa.

Menor: Un riesgo se considera menor cuando el impacto causado por este afecta de manera despreciables los activos de la compañía pero puede ser causante de paralización de procesos de forma temporal.

Insignificante: Un riesgo se considera insignificante cuando compromete de manera despreciable los activos de la compañía, no es causante de paralización de procesos y puede llegar a obviarse.

10.2.2.5.4 VALORACION DE LOS RIESGOS IDENTIFICADOS

No riesgo	Probabilidad de ocurrencia	Consecuencia o costo	Nivel de Riesgo Absoluto
1	Probable	Mayor	Extremo
2	Posible	Mayor	Extremo
3	Posible	Catastrófico	Extremo
4	Probable	Moderado	Alto
5	Posible	Moderado	Alto
6	Probable	Mayor	Extremo
7	Posible	Mayor	Extremo
8	Posible	Moderado	Alto
9	Probable	Mayor	Extremo
10	Posible	Catastrófico	Extremo
11	Probable	Mayor	Extremo

Tabla 5.Valoración de los riesgos identificados

10.2.2.5.5 MAPA DE RIESGOS

	Insignificante	Menor	Moderada	Mayor	Catastrófica
Casi certeza					
Probable			**4, 10**	**8**	**1**
Posible		**7, 11**	**6**	**2**	**3, 9**
Improbable		**5**			
Raro					

Figura 6. Mapa de riesgo

10.2.2.5.6 MATRIZ DE RIESGOS Y CONTROLES

ESCENARIOS	CODIGO DEL RIESGO	RIESGO	DESCRIPCIÓN DEL RIESGO					DESCRIPCIÓN DEL CONTROL			RIESGO RESIDUAL
			PROBABILIDAD	VR.	IMPACTO	VR.	VALORACION DEL RIESGO %	CONTROL	VALORACION DE RIESGO SEGÚN SU PROBABILIDAD LUEGO DEL CONTROL	VALORACION DE RIESGO SEGÚN SU IMPACTO LUEGO DEL CONTROL	
Acceso y seguridad	0001	Inadecuados o ausencia de controles de Seguridad	PROBABLE	38%	CATASTROFICO	51%	89%	Adecuada parametrizacion de los campos del aplicativo	IMPROBABLE	MAYOR	71%
								Existencia de Políticas para la Protección y seguridad de los Datos	POSIBLE	CATASTROFICO	
	0002	Inadecuado definición o Inexistente controles de nivel de acceso al sistema	POSIBLE	29%	MAYOR	42%	71%	Adecuada definición de políticas de roles y perfiles para el acceso a la base de datos	POSIBLE	MAYOR	67%
								Existencia de controles y validación de acceso al sistema	IMPROBABLE	MAYOR	
Base de datos	0003	Pérdida de información debido que el sistema presente inconsistencia en la base de datos	POSIBLE	29%	CATASTROFICO	51%	80%	Existencia de políticas y procedimientos para la administración de la BD	IMPROBABLE	MAYOR	68%
								Existencia de procedimientos y documentación de los cambios que se realicen en la base de datos	POSIBLE	MAYOR	
								Adecuada integridad y consistencia de la base de datos	POSIBLE	MAYOR	
Documentación	0004	Inexistencia o desactualización de documentación del Sistema	PROBABLE	38%	MODERADO	31%	69%	Existencia de Documentación actualizada del sistema (Incluye manuales técnicos- usuario - instalación)	IMPROBABLE	MODERADO	50%
								Documentación de los requerimientos funcionales del sistema.	IMPROBABLE	MENOR	
								Existencia de procedimientos y documentación de los cambios que se realicen en la base de datos	POSIBLE	MODERADO	
Ergonomía	0005	Interfaz de usuario compleja	IMPROBABLE	20%	MENOR	20%	40%	Adecuada capacitación a los usuarios sobre el correcto uso y administración del aplicativo	IMPROBABLE	MENOR	35%
								Apropiado desarrollo del diseño de interfaz de usuario	IMPROBABLE	INSIGNIFICANTE	
Pruebas del software	0006	Ausencia o Inadecuada realización de Pruebas de Software	POSIBLE	29%	MODERADO	31%	60%	Documentación, Ejecución y aceptación de pruebas del aplicativo por parte del usuario	POSIBLE	MENOR	49%
Portabilidad	0007	Inadecuada portabilidad del Sistema	POSIBLE	29%	MENOR	20%	49%	Identificación de la plataforma en donde se va a implementar el aplicativo	IMPROBABLE	MENOR	40%
Trazabilidad del Sistema	0008	Ausencia de Pistas de Auditoria	PROBABLE	38%	MAYOR	42%	80%	Adecuado desarrollo y diseño del aplicativo con facilidad de ser altamente auditable	PROBABLE	MODERADO	69%
Copias de Respaldos (Backup	0009	Ausencia o inadecuada definición de copias de respaldo	POSIBLE	29%	CATASTROFICO	51%	80%	Existencia de Políticas de Respaldo	POSIBLE	MODERADO	64%
								Existencia de un sitio alterno para salvaguardar la información	POSIBLE	CATASTROFICO	
								Existencia de copias de respaldo (Backup)	IMPROBABLE	MODERADO	
Funcionalidad	0010	Inconsistencia en el funcionamiento de los diferentes módulos del aplicativo.	PROBABLE	38%	MODERADO	31%	69%	Existencia de una bitácora de fallas para identificar problemas que presente el aplicativo	POSIBLE	MODERADO	60%
Control de Cambios	0011	Inadecuado o inexistencia de gestión de cambios del aplicativo	POSIBLE	29%	MENOR	20%	49%	Existencia de instrucciones para evitar la entrada no autorizada de cambios en el programa	IMPROBABLE	MENOR	40%
								Existencia de procedimientos de nuevos cambios en el aplicativo	IMPROBABLE	INSIGNIFICANTE	
								Documentación de registros sobre los cambios realizados al aplicativo.	POSIBLE	MENOR	

Figura 7. Matriz de riesgos y controles

10.2.2.5.7 MATRIZ DE RIESGO RESIDUAL

	Insignificante	Menor	Moderada	Mayor	Catastrófica
Casi certeza					
Probable			**8**		
Posible		**6**	**9, 10**	**1**	
Improbable	**5**	**7, 11**	**4**	**2,3**	
Raro					

Figura 8. Matriz de riesgo residual

10.2.3 ACTIVIDADES PROPIAS DE LA AUDITORIA

10.2.3.1 SELECCIÓN DE DOMINIOS, PROCESOS Y OBJETIVOS DE CONTROL COBIT SELECCIONADOS

10.2.3.1.1 DOMINIOS COBIT SELECCIONADOS

Los Dominios seleccionados del marco de referencia COBIT 4.1 para el desarrollo de la auditoria fueron:

PLANEAR Y ORGANIZAR (PO)

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

- ¿Están alineadas las estrategias de TI y del negocio?
- ¿La empresa está alcanzando un uso óptimo de sus recursos?
- ¿Entienden todas las personas dentro de la organización los objetivos de TI?
- ¿Se entienden y administran los riesgos de TI?
- ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio?

ADQUIRIR E IMPLEMENTAR (AI)

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

- ¿Es probable que los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio?
- ¿Es probable que los nuevos proyectos sean entregados a tiempo y dentro del presupuesto?
- ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?
- ¿Los cambios no afectarán a las operaciones actuales del negocio?

ENTREGAR Y DAR SOPORTE (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativos. Por lo general cubre las siguientes preguntas de la gerencia:

- ¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio?
- ¿Están optimizados los costos de TI?
- ¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?

• ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

10.2.3.1.2 PROCESOS COBIT SELECCIONADOS

PO3 - DETERMINAR LA DIRECCIÓN TECNOLOGICA

Objetivo: Aprovechar al máximo de la tecnología disponible o tecnología emergente, satisfaciendo los requerimientos de negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica, tomando en consideración:

- La capacidad de adecuación y evolución de la infraestructura actual, que deberá concordar con los planes a largo y corto plazo de tecnología de información y debiendo abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.
- El monitoreo de desarrollos tecnológicos que serán tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.
- Las contingencias (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura), con lo que se evaluará sistemáticamente el plan de infraestructura tecnológica.
- Planes de adquisición, los cuales deberán reflejar las necesidades identificadas en el plan de infraestructura tecnológica.

PO9 - EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI

Objetivo: Asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI

Para ello se logra la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos y se toma en consideración:

- Identificación, definición y actualización regular de los diferentes tipos de riesgos de TI (por ej.: tecnológicos, de seguridad, etc.) de manera de que se pueda determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable
- Definición de alcances, límites de los riesgos y la metodología para las evaluaciones de los riesgos.
- Actualización de evaluación de riesgos
- Metodología de evaluación de riesgos
- Medición de riesgos cualitativos y/o cuantitativos
- Definición de un plan de acción contra los riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continua.
- Aceptación de riesgos dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de que tan económico resulte implementar protecciones y controles.

PO10 - ADMINISTRAR PROYECTOS

Objetivo: Establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión

Para ello se realiza una identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización. Además, la organización deberá adoptar y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido y se toma en consideración:

- Definición de un marco de referencia general para la administración de proyectos que defina el alcance y los límites del mismo, así como la metodología de administración de proyectos a ser adoptada y aplicada para cada proyecto emprendido. La metodología deberá cubrir, como mínimo, la asignación de responsabilidades, la determinación de tareas, la realización de presupuestos de tiempo y recursos, los avances, los puntos de revisión y las aprobaciones.
- El involucramiento de los usuarios en el desarrollo, implementación o modificación de los proyectos.
- Asignación de responsabilidades y autoridades a los miembros del personal asignados al proyecto.
- Aprobación de fases de proyecto por parte de los usuarios antes de pasar a la siguiente fase.
- Presupuestos de costos y horas hombre
- Planes y metodologías de aseguramiento de calidad que sean revisados y acordados por las partes interesadas.
- Plan de administración de riesgos para eliminar o minimizar los riesgos.

- Planes de prueba, entrenamiento, revisión post-implementación.

AI2 - ADQUIRIR Y MANTENER SOFTWARE APLICATIVO

Objetivo: Proporciona funciones automatizadas que soporten efectivamente al negocio. Para ello se definen declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros y se toma en consideración:

- Requerimientos de usuarios, para realizar un correcto análisis y obtener un software claro y fácil de usar.
- Requerimientos de archivo, entrada, proceso y salida.
- Interface usuario-maquina asegurando que el software sea fácil de utilizar y que sea capaz de auto documentarse.
- Personalización de paquetes.
- Realizar pruebas funcionales (unitarias, de aplicación, de integración y de carga y estrés), de acuerdo con el plan de prueba del proyecto y con los estándares establecidos antes de ser aprobado por los usuarios.
- Controles de aplicación y requerimientos funcionales.
- Documentación (materiales de consulta y soporte para usuarios) con el objeto de que los usuarios puedan aprender a utilizar el sistema o puedan sacarse todas aquellas inquietudes que se les puedan presentar

AI4 – FACILITAR LA OPERACIÓN Y EL USO

Objetivo: Asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas.

Para ello se realiza un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento y toma en consideración:

- Manuales de procedimientos de usuarios y controles, de manera que los mismos permanezcan en permanente actualización para el mejor desempeño y control de los usuarios.
- Manuales de Operaciones y controles, de manera que estén en permanente actualización.
- Materiales de entrenamiento enfocados al uso del sistema en la práctica diaria.

AI5 - ADQUIRIR RECURSOS DE TI

Objetivo: Verificar y confirmar que la solución sea adecuada para el propósito deseado Para ello se realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas y toma en consideración:

- Capacitación del personal de acuerdo al plan de entrenamiento definido y los materiales relacionados.
- Conversión / carga de datos, de manera que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo.

- Pruebas específicas (cambios, desempeño, aceptación final, operacional) con el objeto de obtener un producto satisfactorio.
- Acreditación de manera que la Gerencia de operaciones y usuaria acepten los resultados de las pruebas y el nivel de seguridad para los sistemas, junto con el riesgo residual existente.
- Revisiones post implementación con el objeto de reportar si el sistema proporciono los beneficios esperados de la manera más económica.

AI6 – ADMINISTRAR CAMBIOS

Objetivo: Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores.

Esto se hace posible a través de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual y toma en consideración:

- Identificación de cambios tanto internos como por parte de proveedores
- Procedimientos de categorización, priorización y emergencia de solicitudes de cambios.
- Evaluación del impacto que provocaran los cambios.
- Autorización de cambios
- Manejo de liberación de manera que la liberación de software este regida por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega, etc.

- Distribución de software, estableciendo medidas de control especificas para asegurar la distribución de software correcto al lugar correcto, con integridad y de manera oportuna.

AI7 – INSTALAR Y ACREDITAR SOLUCIONES Y CAMBIOS

Objetivo: Contar con sistemas nuevos o modificados que trabajen sin problemas importantes después de la instalación, Enfocándose en Probar que las soluciones de aplicaciones e infraestructura son apropiadas para el propósito deseado y estén libres de errores, y planear las liberaciones a producción

Esto se logra con:

- El establecimiento de una metodología de prueba
- Evaluar y aprobar los resultados de las pruebas por parte de la gerencia del negocio
- Ejecutar revisiones posteriores a la implantación

DS5 –GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS

Objetivo: salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida

Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración:

- Autorización, autenticación y el acceso lógico junto con el uso de los recursos de TI deberá restringirse a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso
- Perfiles e identificación de usuarios estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario
- Administración de llaves criptográficas definiendo implementando procedimientos y protocolos a ser utilizados en la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas
- Manejo, reporte y seguimiento de incidentes implementado capacidad para la atención de los mismos
- Prevención y detección de virus tales como Caballos de Troya, estableciendo adecuadas medidas de control preventivas, detectivas y correctivas.
- Utilización de Firewalls si existe una conexión con Internet u otras redes públicas en la organización

10.2.3.1.3 OBJETIVOS DE CONTROL SELECCIONADOS

PO3 - DETERMINAR LA DIRECCIÓN TECNOLÓGICA

- PO3.3 Monitoreo de Tendencias y Regulaciones Futuras

PO9 - EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI

- PO 9.3 Identificación de eventos
- PO 9.4 Evaluación de riesgos de TI
- PO 9.5 Respuesta a los riesgos
- PO 9.6 Mantenimiento y monitoreo de un plan de acción de riesgos

PO10 - ADMINISTRAR PROYECTOS

- PO 10.2 Marco de trabajo para la administración de proyectos
- PO 10.5 Declaración del alcance del proyecto
- PO 10.8 Recursos del proyecto
- PO 10.9 Administración de riesgos del proyecto
- PO 10.11 Control de cambios del proyecto

AI2 - ADQUIRIR Y MANTENER SOFTWARE APLICATIVO

- AI 2.3 Control y posibilidad de auditar las aplicaciones
- AI 2.4 Seguridad y disponibilidad de las aplicaciones
- AI 2.10 Mantenimiento de software aplicativo

AI4 – FACILITAR LA OPERACIÓN Y EL USO

- AI 4.3 Transferencia de conocimiento a usuarios finales
- AI 4.4 Transferencia de conocimiento a personal de operaciones y soporte

AI5 - ADQUIRIR RECURSOS DE TI

- AI 5.1 Control de adquisición
- AI 5.4 Adquisición de recursos de TI

AI6 – ADMINISTRAR CAMBIOS

- AI6.1 Estándares y Procedimientos para Cambios
- AI6.3 Cambios de Emergencia
- AI6.4 Seguimiento y Reporte del Estatus de Cambio
- AI6.5 Cierre y Documentación del Cambio

AI7 – INSTALAR Y ACREDITAR SOLUCIONES Y CAMBIOS

- AI7.2 Plan de Prueba
- AI7.3 Plan de Implantación
- AI7.4 Ambiente de Prueba
- AI7.6 Pruebas de Cambios
- AI7.7 Prueba de Aceptación Final
- AI7.9 Revisión Posterior a la Implantación

DS5 – GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS

- DS 5.3 Administración de identidad
- DS 5.4 Administración de cuentas de usuario

10.2.3.2 OBSERVACIONES Y RECOMENDACIONES SOBRE LOS PROCESOS COBIT SELECCIONADOS

PO3 - Determinar la Dirección Tecnológica

OBSERVACIONES

Realizando una entrevista con el gerente general de COMPGENIOSS observó que:

- CompGenioss no cumple con las normas y políticas legales para el desarrollo y la comercialización de MEDUL lo cual puede ser causal de sanciones y penalizaciones.

RECOMENDACIONES

En base a las observaciones encontradas se recomienda:

- Implementar en el menor tiempo posible las normas y políticas legales para el desarrollo y comercialización de MEDULA.
- Se deben asesorar con personas conocedoras de los temas legales, al momento de implementar un nuevo proyecto para que no tengas problemas futuras.

OPINIÓN DEL AUDITOR

Es muy importante destacar el cumplimiento de las legislaciones y regulaciones establecidas por la ley ya que de esta manera se evitaran multas y sanciones, en estos momentos CompGenioss no ha tenido presente el cumplimiento de las mismas, pero todo esto se debe al desconocimiento de este tipo de procesos al momento de entrar en el campo del desarrollo y comercialización de un producto.

PO9 Evaluar y administrar los riesgos de TI

OBSERVACIONES

Realizando una entrevista con el gerente de operación tecnológica se observó que:

- CompGenioss no tiene identificados los riesgos y su ocurrencia, en ninguna etapa del proyecto se realizó una valoración de riesgos.
- No se tiene implementación de un plan de acción de riesgos.

RECOMENDACIONES

En base a las observaciones encontradas se recomienda:

- Realizar un plan de acción de riesgos que pueden presentarse antes, durante y después del desarrollo del proyecto.
- Realizar una adecuada valoración de riesgos la cual valide su probabilidad de ocurrencia y el impacto.
- Llevar al corriente la documentación de eventos y sucesos que se presenten en el ciclo de vida de los proyectos.

OPINIÓN DEL AUDITOR

No se está realizando una debida gestión y documentación para la administración de los riesgos de TI lo cual imposibilita una adecuada respuesta en caso tal de que un riesgo logre materializarse siendo esto causante de pérdidas de dinero, insatisfacción del cliente con los productos adquiridos y perdida de la imagen comercial de la empresa. Por ende se CompGenioss debe ser consciente de la importancia de realizar una adecuada valoración de riesgos de TI antes de emprender el desarrollo de un nuevo aplicativo.

PO10 Administrar Proyectos

OBSERVACIONES

Realizando una entrevista con el gerente general se observó que:

- CompGenioss no cuenta con políticas definidas de cómo se debe realizar el emprendimiento de nuevos proyectos
- Algunos de los proyectos no se logran entregar en el tiempo estipulado en el cronograma
- En algunas ocasiones los costos han sobrepasado el presupuesto establecido para el desarrollo del proyecto.
- No se tienen identificados los riesgos que se pueden presentar en el desarrollo del proyecto
- Cuando se realizan cambio en el cronograma y en el presupuesto estos se están informando al encargado y adicionalmente se les está haciendo su respectiva documentación

RECOMENDACIONES

En base a las observaciones encontradas se recomienda:

- La realización de políticas que sirvan como guías para el desarrollo de nuevos proyectos.
- Tomar medidas adecuadas para el manejo de los recursos entre ellos dinero, personal, equipos de cómputo.
- Realizar una adecuada gestión de riesgos del proyecto para tener documentados las posibilidades de ocurrencia y el impacto con el objetivo de mitigar y prevenir la ocurrencia de los mismos.

OPINIÓN DEL AUDITOR

Es indispensable la creación de una política o marco de trabajo que entre a regir el cómo y

el porqué de la realización de un nueva proyecto de TI, esto debe realizarse con el fin de garantizar excelente resultados y la calidad del mismo; se debe tener presente los riesgos, recursos, pruebas, entregables y costos para el desarrollo con éxito de los proyectos de TI

AI2 Adquirir y mantener software aplicativo

OBSERVACIÓN

Realizando una entrevista con el gerente de operación tecnológica se observó que:

- CompGenioss no ha verificado que MEDULA cumpla con las legislaciones y regulaciones establecidas por la ley lo cual puede ser causal de sanciones y penalizaciones.
- El aplicativo no tiene la posibilidad de ser auditado más sin embargo la base de datos que está realizada en SQL SERVER 2008 si cuenta con esta fortaleza.
- No se ha verificado la seguridad del aplicativo.
- Se les está comentando a los posibles clientes la importancia del cambio de tecnología.

RECOMENDACIONES

En base a las observaciones encontradas se recomienda:

- Verificar que los software desarrollados por CompGenioss entre ellos MEDULA estén cumpliendo y cumplan con las legislaciones y regulaciones establecidas por la ley con el fin de evitar multas y sanciones.
- Se debe verificar la seguridad de los productos tales como controles de accesos, cambio de contraseñas, longitud de las contraseñas, fortaleza de las contraseñas, etc.

OPINIÓN DEL AUDITOR

Es muy importante destacar el cumplimiento de las legislaciones y regulaciones establecidas por la ley ya que de esta manera se evitaran multas y sanciones, en estos momentos CompGenioss no ha tenido presente el cumplimiento de las mismas y lamentablemente MEDULA no cuenta con un módulo de auditoría pero si existe la posibilidad de auditar el motor de base de datos utilizado por MEDULA el cual es SQL SERVER 2008. De momento no se estaban revisando los controles de acceso al aplicativo lo cual es que lo que brinda la seguridad para la protección de uno de los activos más importantes para cualquier organización la información.

AI4 Facilitar la operación y el uso

OBSERVACIONES

Realizando una entrevista con el gerente general se observó que:

- El aplicativo MEDULA no cuenta con manuales de usuarios para el uso del sistema y de igual forma no cuenta con los manuales de operaciones y soporte, para la configuración y mantenimiento del aplicativo o algún documento formal que pueda servir de ayuda para el cliente.

RECOMENDACIONES

En base a las observaciones encontradas se recomienda:

- La creación de manuales de usuarios para el aplicativo MEDULA con el fin de que el personal actual y futuro tenga una base de ayuda y guía, al momento de solucionar un inconveniente en algún proceso de la aplicación, además de ayudar en la realización de las tareas diarias del usuario.
- La creación de los manuales de operaciones y soporte del aplicativo MEDULA, para que se puedan realizar de forma correcta y segura todas las instalaciones,

configuraciones y mantenimientos necesarios.

- Complementar la realización y entrega de los manuales, con capacitaciones periódicas, sobre el uso efectivo de todos los recursos de la herramienta, tanto a nivel de usuario final como a nivel de operaciones y soporte.

OPINIÓN DEL AUDITOR

CompGenioss se encuentra incumpliendo, uno de los requerimientos más importantes al momento de realizar y entregar un aplicativo, y es que no está transmitiendo al cliente la información necesaria para que este opere de forma segura y ágil el nuevo producto adquirido, ya sea por medio de manuales, documentos formales o capacitaciones, lo cual propiciara a futuro inmediato fallas y errores en el aplicativo, debido al desconocimiento del funcionamiento y configuración del nuevo sistema.

AI5 Adquirir recursos de TI

OBSERVACIONES

Realizando una entrevista con el gerente de operación tecnológica se observó que:

- CompGenioss no cuenta con procesos y políticas definidas para la adquisición de recursos de TI, solo se realiza una investigación de mercado y se selecciona la que mejor se ajuste a las necesidades de la empresa basándose sobre todo en la marca y en el precio.
- No se está documentando el registro de los recursos de TI que adquiere la organización.
- Cuando se adquieren nuevos recursos de TI no se les realiza capacitación a los empleados únicamente les comentan sobre la tecnología adquirida.
- Para la adquisición de recursos de TI se cuenta con la aprobación del Gerente

General el señor Bladimir Cahuana.

RECOMENDACIONES

En base a las observaciones encontradas se recomienda:

- Se debe crear políticas para la adquisición de recursos de TI en las cuales se documente y se resalte una descripción detallada de los recursos adquiridos tal como la fecha de adquisición, marca, precio, proveedores, competencia en el mercado.
- Se debe de realizar una documentación sobre los recursos de TI adquiridos así como también los nuevos adquirir con el objetivo de llevar un control exhaustivo sobre estos activos que son sumamente importante para la organización.
- Al momento de adquirir una nueva tecnológica se debe capacitar a los empleados sobre el producto adquirido brindándole la oportunidad de entender sus funcionamiento, funcionalidad así como de resolver sus dudas e inquietudes.

OPINIÓN DEL AUDITOR

CompGenioss en estos momentos está realizando una inadecuada gestión para la adquisición de recursos de TI ya que no cuenta con una política definida para dicha gestión simplemente se apoyan en el reconocimiento de la marca o el precio del producto adicionalmente no se están realizando las capacitaciones pertinentes para las tecnologías adquiridas, sin embrago para la adquisición de tecnología se cuenta con la autorización previa del gerente general.

AI6 Administrar Cambios

OBSERVACIONES

Realizando una entrevista con el gerente general se observó que:

- CompGenioss no cuenta como un procedimiento formal ni con una autorización previa para realizar cambios en el aplicativo
- No se tiene documentado el manual de usuario, solo se le hacen las pruebas para probar pero no se documenta nada

RECOMENDACIONES

En base a las observaciones encontradas se recomienda:

- Establecer políticas y procedimientos formales para la administración de cambios en el aplicativo
- Establecer un proceso formal para autorizar los cambios de emergencia que no sigan el proceso de cambio establecido
- Documentar el manual de usuarios del aplicativo y actualizarlo cada vez que se realice un cambio en la aplicación

OPINIÓN DEL AUDITOR

En CompGenioss la administración de cambios en el aplicativo MEDULA es aceptable, debido a que no existe un proceso de administración de cambio informal, no existe autorización previa para realizar cambios, no se tiene conciencia de que el cambio puede causar una interrupción para TI y las operaciones de negocio, no se cuenta con procedimientos que sean utilizados para manejar todos los cambios de forma eficiente y rápida.

AI7 Instalar y Acreditar Soluciones y Cambios

OBSERVACIONES

Realizando una entrevista con el gerente general se observó que:

- No se establece un plan de pruebas ni ambiente de prueba; Las pruebas las realiza el desarrollador según su criterio en el momento en el que él las indique
- Algunas veces se evalúan y se aprueban los resultados de las pruebas por parte de la gerencia de la compañía
- Cuando se realizan los cambios se le hace una revisión posterior a la implantación

RECOMENDACIONES

En base a las observaciones encontradas se recomienda:

- Establecer un plan y un ambiente de prueba, y que este sea aprobado por las partes relevantes de la organización
- Se debe asegurar que el dueño del proceso de negocio y los interesados de TI evalúen los resultados de los procesos de pruebas
- Realizar revisiones post implementación a los cambios realizados al aplicativo

OPINIÓN DEL AUDITOR

La instalación y acreditación de soluciones y Cambios en la organización es aceptable, debido a que las soluciones se identifican de manera informal con base en la experiencia de los desarrolladores, ellos son los que realizan las pruebas en el momento en el que él las indique ya que no existe un procedimiento formal a seguir dentro de la compañía. Se usan enfoques no estructurados para definir los requerimientos e identificar las soluciones tecnológicas y cambios. En ocasiones la gerencia reconoce la necesidad de verificar que las soluciones se ajustan para el propósito deseado.

DS5 Garantizar la seguridad de los sistemas

OBSERVACIONES

Revisando el funcionamiento del sistema MEDULA se observó que:

- Las cuentas de los usuarios del aplicativo, tienen roles y perfiles similares, lo cual no permite identificar cual es el usuario administrador del aplicativo y cual es un usuario con privilegios restringidos.

HALLAZGOS:

- En el tipo de usuario "Normal", al momento de seleccionar, cualquier opción de los menús, del módulo de consulta externa, el sistema muestra un mensaje de "EL USUARIO NO ESTA AUTORIZADO PARA EJECUTAR ESTA OPCIÓN", lo cual indica que no debería de tener acceso al formulario, pero al cerrar el mensaje, se despliega el formulario solicitado.

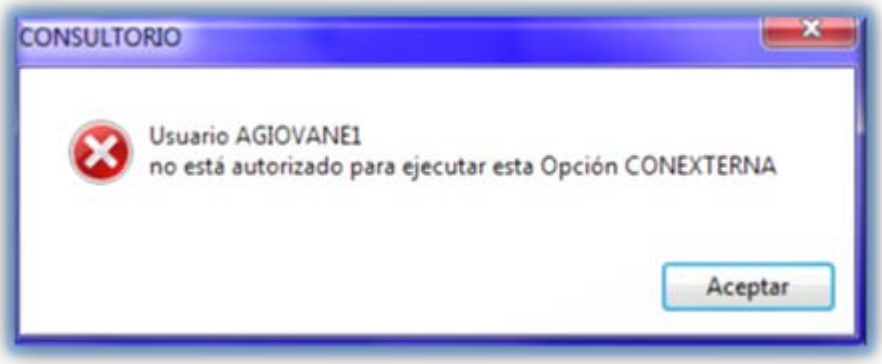
- Al momento de ingresar un nuevo registro de paciente, en la casilla de identificación, el aplicativo permite que se ingresen letras, símbolos además de los números, que son los únicos que deben de estar permitidos digitar en este campo, después de ingresar la identificación, (errónea o correcta) el aplicativo no permite modificar este campo, y permite diligenciar el resto del formulario, y hace como si lo hubiese guardado en la base de datos, pero al revisar en la lista de pacientes, este no se encuentra guardado.

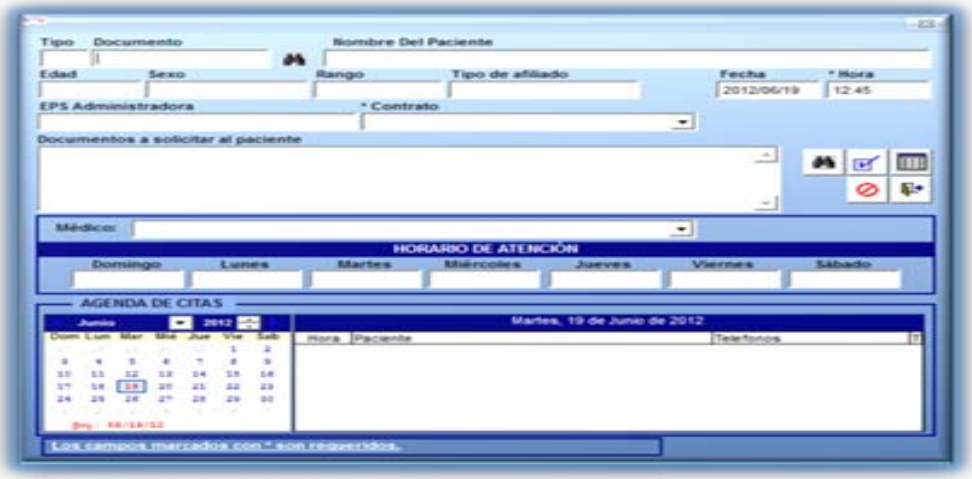
- Al momento de realizar la búsqueda de un paciente para anular la cita, la búsqueda por nombre falla, solo busca por medio del código del paciente.

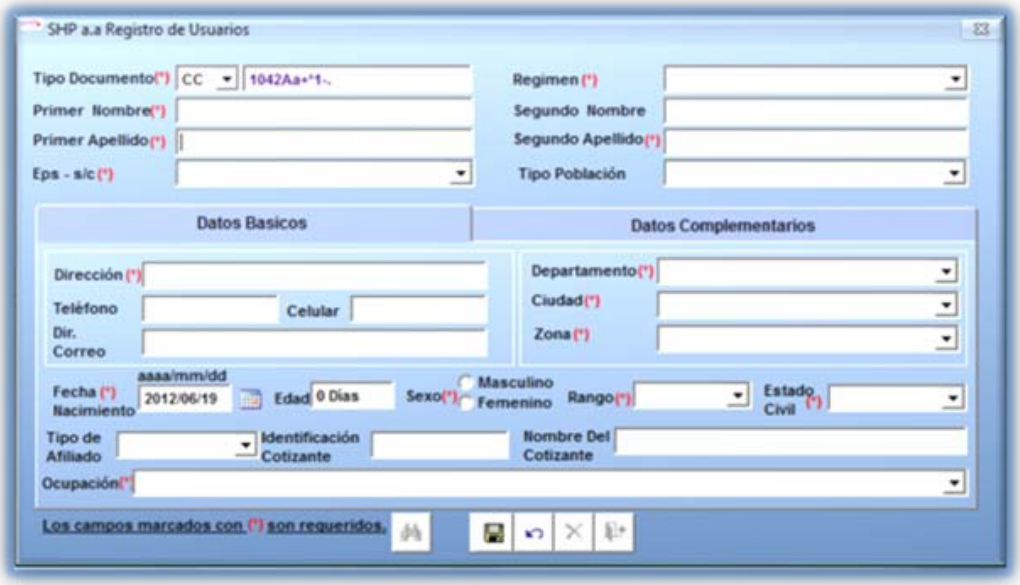
- Hay pacientes a quien se les asignan citas médicas, aun cuando el contrato con EPS, ha finalizado, en algunos casos, hasta en más de un año.

- Al momento de tratar de ingresar al sistema, por medio de claves erradas, se observa que el número de intentos fallidos permitidos es de dos, luego el sistema arroja un mensaje de “Demasiados intentos con claves erróneas”.

EVIDENCIAS:





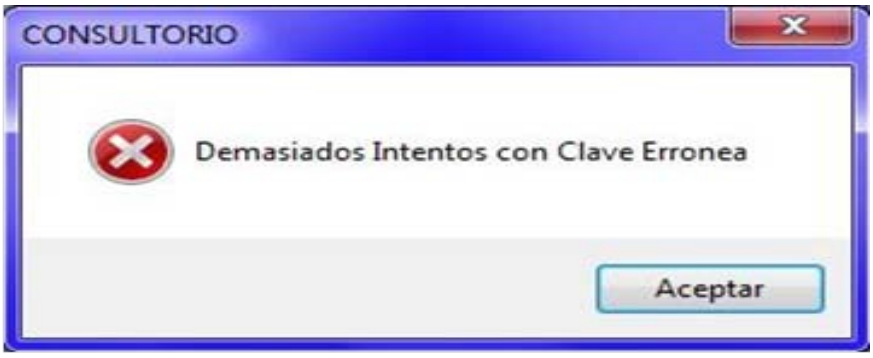

SHP a.a Registro de Usuarios
Tipo Documento(*)
CC
1042Aa+*1-.
Regimen (*)
Primer Nombre(*)
Segundo Nombre
Primer Apellido(*)
Segundo Apellido(*)
Eps - s/c (*)
Tipo Población
Datos Basicos
Datos Complementarios
Dirección (*)
Teléfono
Celular
Dir. Correo
Departamento(*)
Ciudad (*)
Zona (*)
Fecha (*) Nacimiento
aaaa/mm/dd
2012/06/19
Edad
0 Dias
Sexo(*)
Masculino
Femenino
Rango(*)
Estado Civil (*)
Tipo de Afiliado
Identificación Cotizante
Nombre Del Cotizante
Ocupación(*)
Los campos marcados con (*) son requeridos.


18 7212345 CC FAUSTO GONZALEZ PEREZ 1945-05-16 M 3 B+
19 789455+ 72192909 CC DASD ASD ASD 1927-06-28 M 1 O+


Anular Citas
Buscar por:
Criterio de búsqueda
Código
7212345
Doc. Paciente
Nombre Paciente
Fecha Cita
Hora Cita
Tipo de Cita
CONSULTORIO
No hay información de citas para anular.
Aceptar
Médico tratante:
Anular por:
Estado de la cita:


Maestro de Convenios
Código Conve.
Empresa
Tarifa
Año
201040
EPS017
FAMISANAR EPS
ISS
2001
Nombre Convenio
TARIFA-ISS 2001 PLENA
Valor Total del Convenio
No. de Usuarios del Convenio
Fecha Vigencia
Fecha Vencimiento
% Aplicado
25,000,000
650
2010/10/01 12:0
2011/12/31 12:00
0.00
Suma
Resta
Texto que Quiere que Aparezca en la Factura
FACTURACION SEGUN CONVENIO 201040, PARA LA ATENCION DE NIÑOS EN LA EDAD DE 5 A 16 AÑOS, CONTRATO VIGENTE HASTA EL 31 DE DICIEMBRE DEL 2010
Cód Convenio
Código EPS
Nombre
Fecha Vig.
Fecha Ven.
Valor Total
Total Usua.
%
Clas
Tarifa
Año
01020504 EPS017 TARIFA-SOAT 2004 PLENA 2010/10/31 2012/12/31 99,500,000,000 580 .00 2 002 2004
10840 EPS017 TARIFA-002 2004 2010/10/01 2011/12/31 800,000 400 5.00 1 002 2004
16547 EPS017 TARIFA - ISS 2010 MAS UN 2 % 2010/10/22 2011/12/31 30,000,000 450 2.00 1 001 2010
201040 EPS017 TARIFA-ISS 2001 PLENA 2010/10/01 2011/12/31 25,000,000 650 .00 0 001 2001
504060 EPS020 TARIFA - ISS 2001 MAS UN 15 % 2010/10/01 2011/12/31 150,000,000 300 15.00 1 001 2001


CONSULTORIO
Clave de Acceso Erronea. Reintente.
Aceptar



RECOMENDACIONES

En base a las observaciones encontradas se recomienda:

- La realización de una matriz de roles y perfiles, para segregar de forma adecuada y segura los permisos y privilegios que tienen los usuarios en el sistema.
- Contar con un debido proceso, para la adecuada definición de roles y perfiles de los usuarios del sistema y de igual forma registrar todos estos procedimientos en dicha matriz.

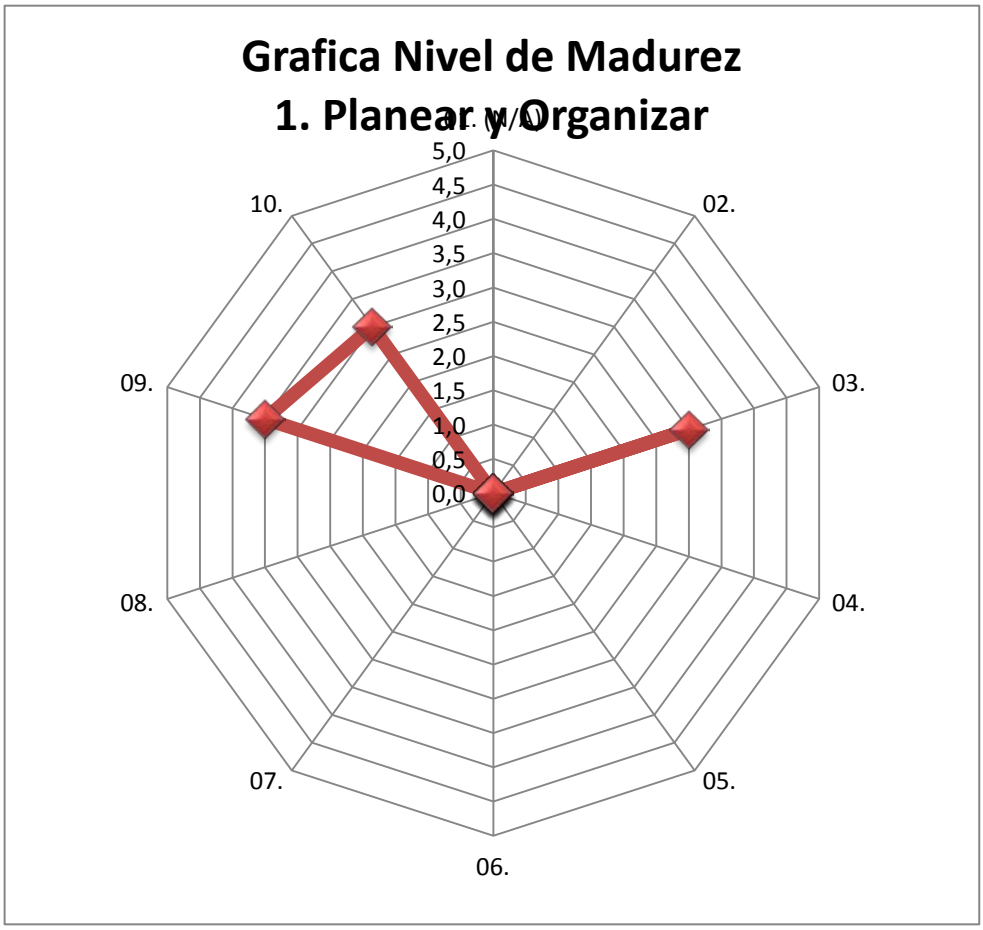
OPINIÓN DEL AUDITOR

En estos momentos el aplicativo MEDULA, se encuentra con una falla grave de seguridad, a nivel de acceso, debido a que no se tiene establecido de forma correcta los permisos y privilegios de todos los usuarios que manejan el sistema, lo que genera riesgo en el manejo, integridad y seguridad de la información. Esta falla debería ser solucionada lo antes posible, puesto que la clave de un buen sistema es la seguridad y el aplicativo MEDULA, tiene muchas deficiencias en esta área.

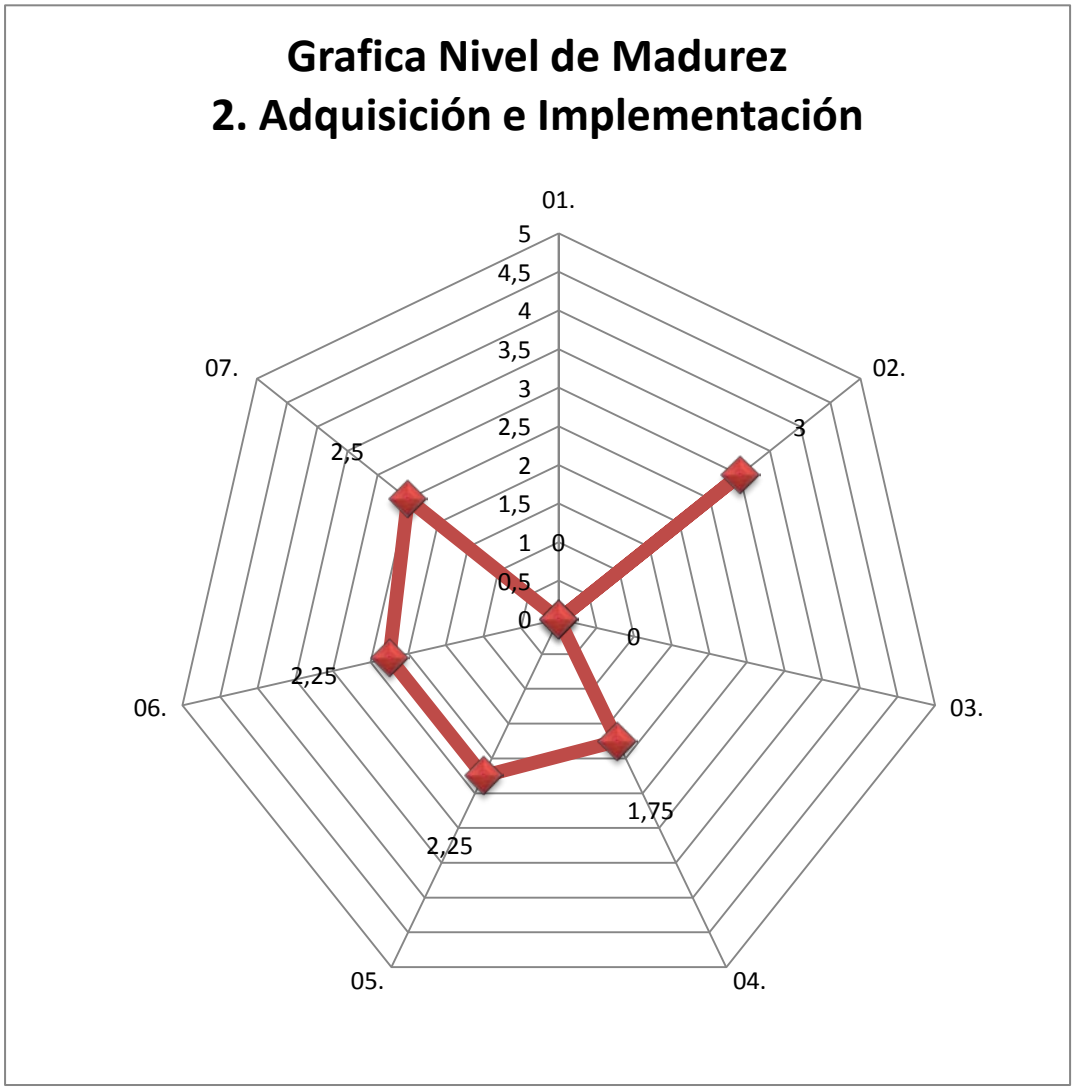
10.2.3.2.1 NIVEL DE MADUREZ DE LOS PROCESOS

El nivel de madurez definido en el marco de referencia COBIT nos indica que también se están administrando los procesos de TI en la organización, de esta forma se puede identificar donde se encuentra la empresa y hacia dónde quiere llegar. Esta auditoría se basó en 3 procesos COBIT planear y organizar, adquirir e implementar y entregar y dar soporte de los cuales se calculó el nivel de madurez inicial y el nivel de madurez que se pretende alcanzar.

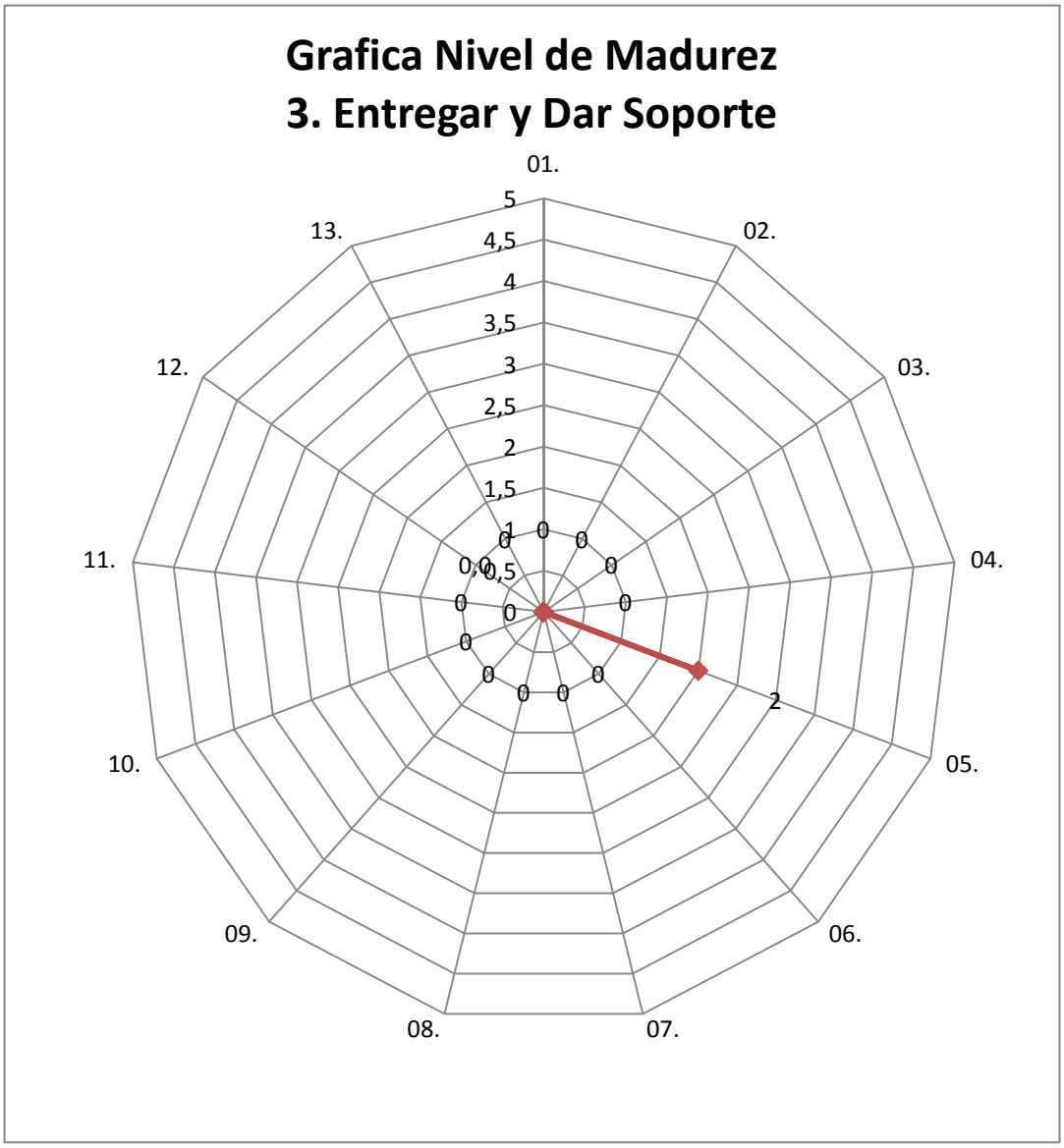
10.2.3.2.1.1 PLANEAR Y ORGANIZAR



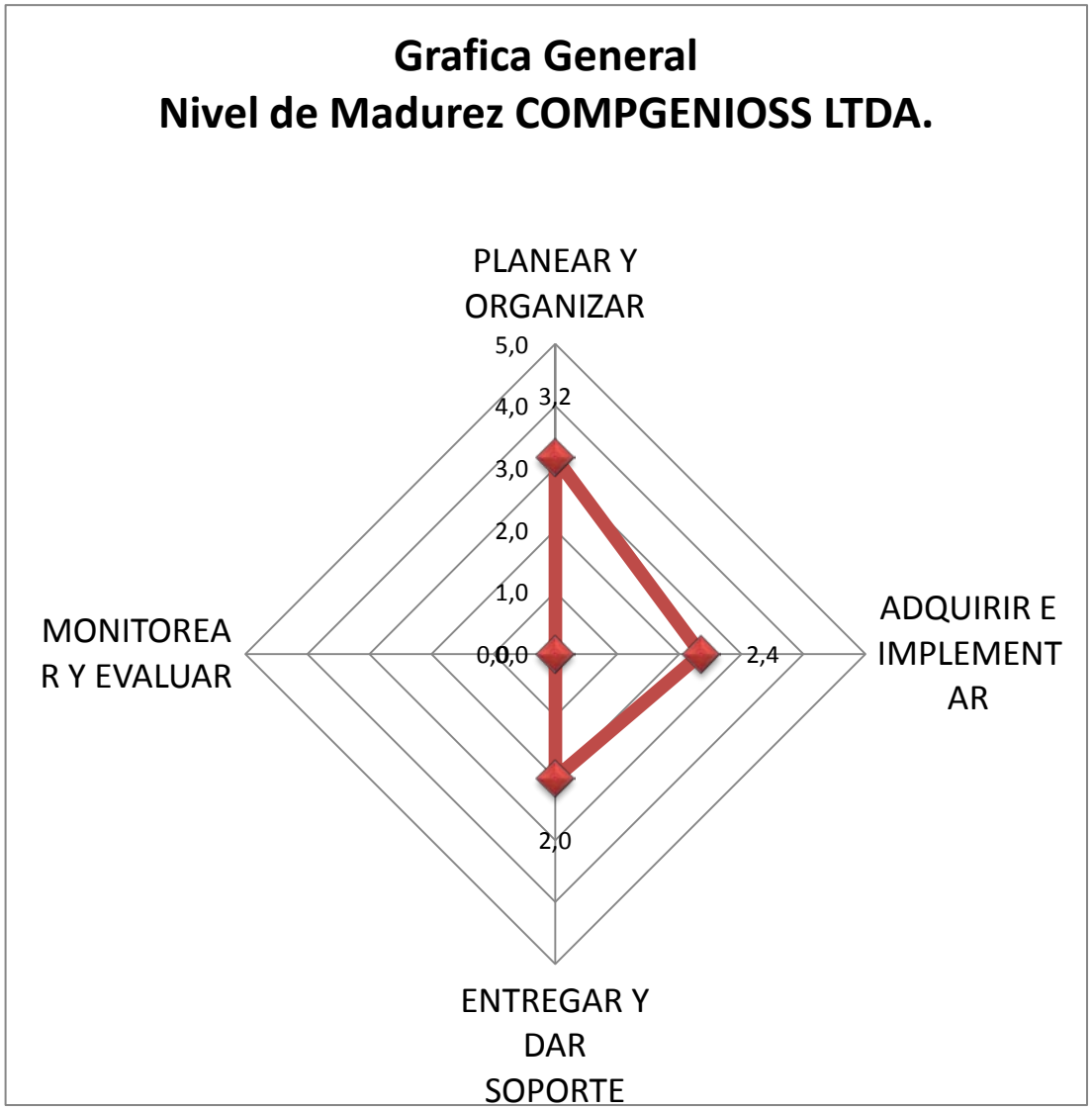
10.2.3.2.1.2 ADQUIRIR E IMPLEMENTAR



10.2.3.2.1.3 ENTREGAR Y DAR SOPORTE



10.2.3.2.2 NIVEL DE MADUREZ GENERAL



En estos momentos podemos observar que el nivel de madurez actual, es «Inicial» y La meta de CompGenioss es llegar a un nivel Entre proceso definido y administrable y medible, con el fin de brindar a sus actuales y futuros clientes un producto soportado y basado en las mejores prácticas.

10.2.3.2.3 RECOMENDACIONES Y BUENAS PRÁCTICAS

Realizada la auditoria al módulo de consulta externa del aplicativo MEDULA, el cual se evaluó aplicando diferentes métodos de detección de riesgos y fallas y de acuerdo a los resultados obtenidos, se le sugiere a la compañía, una serie de recomendaciones y buenas prácticas, que permitirán mejoras en las áreas de manejo de la información, seguridad, procedimientos, control interno y organización:

- Realizar una matriz de roles y perfiles, para segregar de forma adecuada y segura los permisos y privilegios que tienen los usuarios en el sistema.
- Contar con un debido proceso, para la adecuada definición de roles y perfiles de los usuarios del sistema y de igual forma registrar todos estos procedimientos en dicha matriz.
- Verificar que los software desarrollados por CompGenioss entre ellos MEDULA estén cumpliendo y cumplan con las legislaciones y regulaciones establecidas por la ley con el fin de evitar multas y sanciones.
- Se debe verificar la seguridad de los productos tales como controles de accesos, cambio de contraseñas, longitud de las contraseñas, fortaleza de las contraseñas, etc.
- La creación de manuales de usuarios para el aplicativo MEDULA con el fin de que el personal actual y futuro tenga una base de ayuda y guía, al momento de solucionar un inconveniente en algún proceso de la aplicación, además de ayudar en la realización de las tareas diarias del usuario.
- La creación de los manuales de operaciones y soporte del aplicativo MEDULA, para que se puedan realizar de forma correcta y segura todas las instalaciones, configuraciones y mantenimientos necesarios.

- Complementar la realización y entrega de los manuales, con capacitaciones periódicas, sobre el uso efectivo de todos los recursos de la herramienta, tanto a nivel de usuario final como a nivel de operaciones y soporte.
- Se debe crear políticas para la adquisición de recursos de TI en las cuales se documente y se resalte una descripción detallada de los recursos adquiridos tal como la fecha de adquisición, marca, precio, proveedores, competencia en el mercado.
- Se debe de realizar una documentación sobre los recursos de TI adquiridos así como también los nuevos adquirir con el objetivo de llevar un control exhaustivo sobre estos activos que son sumamente importante para la organización.
- Al momento de adquirir una nueva tecnológica se debe capacitar a los empleados sobre el producto adquirido brindándole la oportunidad de entender sus funcionamiento, funcionalidad así como de resolver sus dudas e inquietudes.
- Establecer políticas y procedimientos formales para la administración de cambios en el aplicativo
- Establecer un proceso formal para autorizar los cambios de emergencia que no sigan el proceso de cambio establecido
- Establecer un plan y un ambiente de prueba, y que este sea aprobado por las partes relevantes de la organización.
- Realizar revisiones post implementación a los cambios realizados al aplicativo.
- Realizar un plan de acción de riesgos que pueden presentarse antes, durante y después del desarrollo del proyecto.
- Realizar una adecuada valoración de riesgos la cual valide su probabilidad de ocurrencia y el impacto.
- Llevar al corriente la documentación de eventos y sucesos que se presenten en el ciclo de vida de los proyectos.

- La realización de políticas que sirvan como guías para el desarrollo de nuevos proyectos.
- Tomar medidas adecuadas para el manejo de los recursos entre ellos dinero, personal, equipos de cómputo.
- Realizar una adecuada gestión de riesgos del proyecto para tener documentados las posibilidades de ocurrencia y el impacto con el objetivo de mitigar y prevenir la ocurrencia de los mismos.
- Documentar el manual de usuarios del aplicativo y actualizarlo cada vez que se realice un cambio en la aplicación.
- Se debe asegurar que el dueño del proceso de negocio y los interesados de TI evalúen los resultados de los procesos de pruebas.

CONCLUSIÓN

De acuerdo a la auditoría realizada al módulo de consulta externa del aplicativo MEDULA y a partir de los resultados obtenidos, se concluye que después de evaluar la totalidad de los procesos y funcionalidad del módulo de consulta externa, se encontró que existen fallas en la asignación de roles y perfiles a usuarios en el sistema, lo cual representa un alto riesgos, sobre el manejo de la información y en la seguridad del aplicativo.

También se encontraron fallas en el correcto funcionamiento de diferentes procesos del aplicativo, lo que genera inconsistencia y dudas en la veracidad de la información que se maneja en todo el aplicativo.

Otro factor relevante es la no existencia de documentación formal o manuales de usuario y soporte, debido a esta falla, los resultados al momento de manejar, administrar y dar soporte al aplicativo son preocupantes, puesto que no tienen la correcta capacitación y guías que permitan un eficiente manejo del sistema.

La alineación del proyecto MEDULA, con COBIT 4.1, ITIL V3, ISO 27001 e ISO 3100 y la implementación de buenas prácticas, pretenden encontrar un punto de equilibrio en donde el riesgo disminuya considerablemente y los controles existentes e implementados tengan una mayor efectividad, permitiendo así mejoras en los procesos y que al final se verán reflejados en el nivel de madurez de cada uno de estos.

11. EJECUCIÓN DE LA AUDITORIA

11.1 PLAN DE AUDITORIA

COMPGENIOSS LTDA.
PLAN DE AUDITORIA

OBJETIVO: Realizar una auditoría al sistema de información MEDULA, en el módulo de consulta externa para identificar posibles riesgos y proponer alternativas de solución a la empresa.	
Auditoria N° 01	**ALCANCE DE LA AUDITORIA:**
Duración de la Auditoria: Dos (2) Meses	• Se evaluaran las funciones y procesos, del aplicativo MEDULA, en el módulo de Consulta Externa. Revisando la funcionalidad, rendimiento y controles implantados. • Se evaluará la Base de Datos del aplicativo MEDULA, en donde se revisara la integridad, seguridad y confiabilidad de los datos que se almacenaran en la misma. • Se evaluarán los niveles de seguridad del módulo de Consulta Externa del aplicativo MEDULA, (Control de Acceso, Procesamiento de Datos e Integridad).

			Reunión de Apertura		
Actividad / Proceso	**Documentos**	**Auditores**	**Responsable Proceso**	**Fecha**	**Hora**
Análisis del esquema de funcionamiento del aplicativo MEDULA, específicamente en el módulo de Consulta Externa.	Manuales técnicos y de Usuarios	Irleth Fonseca Alcides Giovannetti José Luis Redondo	Coordinador de Sistemas	26/04/2012	11:00 a.m.
Identificación y evaluación de riesgos potenciales de tecnología de información, específicamente en el módulo de Consulta Externa del aplicativo MEDULA.	Encuestas y Entrevistas.	Irleth Fonseca Alcides Giovannetti José Luis Redondo	Gerente	02/05/2012	05:00 p.m.
Análisis y evaluación de controles y seguridades, atraves de la tecnica de EVALUACIÓN DE CONTROLES, al aplicativo MEDULA, en el módulo de Consulta Externa.	Listas de Chequeo	Irleth Fonseca Alcides Giovannetti José Luis Redondo	Cordinador de Sistemas	08/05/2012	03:00 p.m.

Aplicación de pruebas de auditoría y obtención de evidencias.	Papeles de Trabajo	Irleth Fonseca Alcides Giovannetti José Luis Redondo	Coordinador de Sistemas	04/06/2012	05:00 p.m.
Documentación del trabajo y elaboración del informe final.	Informe Final	Irleth Fonseca Alcides Giovannetti José Luis Redondo	Gerente Coordinador de Sistemas	12/07/2012	10:00 a.m.

NOTA: Para todas las auditorias se debe evaluar el cumplimiento de los requisitos que se van a auditar siguiendo el ciclo PHVA.

Auditor Líder: _____

Nombre y Firma

Auditado: _____

Nombre y Firma

Tabla 6. Plan de auditoria

11.2 CARTA DE INICIO

COMPAÑÍA DE AUDITORIA AIJ LTDA.

Barranquilla, 12 de Marzo de 2012

Ing.

Bladimir Cahuana

Gerencia General CompGenioss LTDA.

E. S. M

REF: Auditoria de sistemas y seguridad al Módulo de consulta externa del aplicativo Medula de la Compañía CompGenioss LTDA.

Damos inicio a la auditoría en referencia, en el período de tiempo comprendido del 4 de Mayo al 3 de Agosto del presente año; la cual será desarrollada por los auditores: Alcides Giovannetti, Irleth Fonseca y José Luis Redondo.

A continuación describimos el objetivo, alcance y los requerimientos de información requeridos al inicio de la misma:

Objetivos.

- ✓ Realizar una auditoría al sistema de información MEDULA, en el módulo de consulta externa o consultorio para identificar posibles riesgos y proponer alternativas de solución a la empresa.
- ✓ Realizar un análisis para determinar las causas de riesgo que pueden presentarse e impedir el correcto funcionamiento del aplicativo MEDULA o comprometer la seguridad de la información.
- ✓ Verificar los controles existentes del módulo de consulta externa en el aplicativo MEDULA y complementarlos de ser necesario.
- ✓ Determinar el nivel de madurez del aplicativo medula utilizando como apoyo el marco de referencia COBIT.
- ✓ Verificar la seguridad, la integridad, y el procesamiento de los datos del aplicativo MEDULA

Alcance

- ✓ Se evaluará las funciones y procesos del aplicativo MEDULA, en el módulo de Consulta Externa. Revisando así la funcionalidad, rendimiento, seguridad y controles implementados.
- ✓ Se evaluará la Base de Datos del aplicativo MEDULA, en donde se revisara la integridad, seguridad y confiabilidad de los datos que se almacenaran en la misma. Entre el 4 de Mayo y el 3 de Agosto del presente año.
- ✓ Se Verificaran la seguridad, la integridad, y el procesamiento de datos del aplicativo MEDULA. Entre el 4 de Mayo y el 3 de Agosto del presente año.

Requerimientos:

- ✓ Documentación del proceso de desarrollo de Software del módulo de Consulta Externa.
- ✓ Pruebas Unitarias realizadas a los diferentes componentes del módulo de Consulta Externa.
- ✓ Pruebas funcionales realizadas al módulo de Consulta Externa y las certificaciones de estas.
- ✓ Set de Pruebas realizadas al módulo de Consulta Externa.
- ✓ Reporte de Usuarios de la aplicación y de Base de Datos.
- ✓ Manuales de Usuarios de la aplicación.
- ✓ Manuales Técnicos de la aplicación.
- ✓ Matriz de roles y perfiles.
- ✓ Esquema de la Base de Datos del aplicativo MEDULA.

Agradecemos de antemano su colaboración,

Cordialmente,

Alcides Giovannetti Cahuana
Auditor de Sistemas
CC. 1.042.349.216 S/grande

Irleth Fonseca Zambrano
Auditora de Sistemas
CC. 1.043.001.010 S/larga

José Redondo Aguilar
Auditor de Sistemas
CC. 1.129.513.615 B/quilla

11.3 LISTA DE CHEQUEO

COMPGENIOSS LTDA.

Lista de Chequeo

Fecha: 10 de Mayo de 2012

Auditores: ALCIDES DE JESÚS GIOVANNETTI CAHUANA
IRLETH KARINE FONSECA ZAMBRANO
JOSE LUIS REDONDO AGUILAR

Auditoria: Al Modulo de Consulta Externa del Sistema De Información Medula De La Empresa Compgenioss Ltda

Item	Requerimiento	Cumple			Observaciones	Soportes
		SI	NO	N/A		
1	La compañía definió políticas sobre riesgos y controles en todos los niveles de sus operaciones y éstas son modificadas de acuerdo con las necesidades?		X			Entrevista con el gerente general
2	Los procesos están documentados y se revisan de forma permanente para actualizarlos y mejorarlos?		X			
3	Existen manuales técnicos de la aplicación?		X			

4	Existe un usuario administrador custodia?	X			El administrador en custodia de la base de datos está a cargo de Carlos Novoa	
5	Se cuenta con una bitácora de fallas del aplicativo?		x			
6	Los cambios se que le hacen al aplicativo se encuentran documentadas?		x		No se documentada nada	
7	Se cuenta con manuales de usuarios de la aplicación?		x			
8	Existe manuales de instalación del aplicativo?		x			
9	Se cuenta con un set de pruebas?		x		Las pruebas las realiza el desarrollador según su criterio en el momento que el indica. Las pruebas que se realizan, al aplicativosolo se hacen en el momento para probar, pero no se documenta, nada.	
10	Existe usuarios de pruebas?		x			

11	Se tiene protección contra la introducción de código malicioso en la base de datos?	x			La protección que se tiene, es la que brinda SQL server 2008	
12	Existe el uso del password para ingresar al aplicativo?	x				
13	El software tiene la capacidad para recuperarse de fallas y/o errores?		x			
14	Se tienen metodologías para el diseño de BD?	x			No se encuentran documentadas, las metodologías para el diseño de la bases de datos.	
15	Existen políticas establecidas para la protección y seguridad de los datos?		x			
16	Existen instrucciones adecuadas para evitar la entrada no autorizada de cambios en el programa?		x			
17	Se tienen establecidos procedimientos de nuevos cambios en la BD?		x			
18	El software cuenta con una interfaz amable?	x				
19	Existe políticas para el uso correcto del software?		x			
20	Se encuentra implementada una versión de prueba del aplicativo en otras compañías?	x			No se encuentra ninguna documentación relacionada a esto.	

21	Existe una norma o estándar alineado al proceso de desarrollo de Software en la organización?		x			
22	Todos los campos del aplicativo se encuentran debidamente parametrizados?	X			la parametrización en el aplicativo es de más o menos un 70%	
23	Existen usuarios genéricos en la base de datos?	X			el usuario que tiene por defecto la base de datos de SQL server 2008	

Tabla 7. Lista de chequeo

Firma de los Auditores de Sistemas:

Alcides Giovannetti Cahuana
CC. 1.042.349.216 S/grande

Irleth Fonseca Zambrano
CC. 1.043.001.010 S/larga

José Luis Redondo Aguilar
CC. 1.129.513.615 B/quilla

11.4 ENTREVISTAS REALIZADAS EN BASE A LOS PROCESOS COBIT SELECCIONADOS

UNIVERSIDAD DE LA COSTA

ENTREVISTAS

AUDITORIA AL MODULO DE CONSULTA EXTERNA DEL SISTEMA DE INFORMACIÓN MEDULA DE LA EMPRESA COMPGENIOSS LTDA.

Ingeniero: Bladimir Cahuana

Julio de 2012

ENTREVISTAS REALIZADAS EN BASE A LOS PROCEOS COBIT SELECCIONADOS

OBJETIVO DE CONTROL: PO3 Determinar la Dirección Tecnológica

Se realizó una entrevista con el gerente de operación tecnológica.

1- Compgenioss, cumple con todas las normas legales para la realización y comercialización de un producto como MEDULA?

Actualmente la empresa, no cuenta con todas las normas y políticas legales para el desarrollo y la comercialización de MEDULA, la gerencia tiene identificado esta falencia y ya se están tomando todas las medidas, para que no existan problemas a futuro.

OBJETIVO DE CONTROL: PO9 Evaluar y administrar los riesgos de ti

Se realizó una entrevista con el gerente de operación tecnológica.

1- Se Tienen identificados los eventos, riesgos, vulnerabilidad que se pueden presentar al momento de implementar el aplicativo en un ambiente de producción?

Para el aplicativo Medula no se tienen identificados de manera formal los posibles incidentes pero se tiene una idea de los posibles problemas que se puedan presentar.

2- Se evalúa la posibilidad y ocurrencia de los riesgos que puede presentar el aplicativo?

Se realizan pruebas de software pero no la ocurrencia de los riesgos.

3- Se cuenta con un plan de acción de riesgos?

No se tiene implementado un plan de acción de riesgos.

OBJETIVO DE CONTROL: PO10 Administrar proyectos

Se realizó una entrevista con el gerente general

1 - CompGenioss cuenta con una política documentada sobre como emprender un nuevo proyecto?

No se cuenta con políticas definidas

2 - CompGenioss ofrece a sus empleados formación sobre los proyectos?

Luego de que se emprende un nuevo proyecto se le ofrece a los empleados charlas y solución de inquietudes.

3 - Los proyectos emprendidos por CompGenioss se logran entregar a tiempo?

En algunas ocasiones se cumple con los tiempos de entrega sin embargo algunos no se entregan en el tiempo deseado

4 - Los costos de la realización de un proyecto se mantienen dentro del presupuesto establecido?

En algunas ocasiones los costos han sobrepasado el presupuesto que se estableció para la realización del proyecto.

5 - Se tiene documentado del alcance de cada proyecto?

Si se definen previamente en un documento formal lo que es el alcance y los objetivos del proyecto.

6 - Cuando surgen cambio en el cronograma o presupuesto del proyecto son debidamente documentados?

Si se informan y documentan los cambios que se realizan en el presupuesto y se informa cualquier otro cambio que surja durante el desarrollo del proyecto.

7 - Antes de emprender un nuevo proyecto se identifican los riesgos que podían presentarse?

CompGenioss no cuenta con un documento en el cual estén definidos los riesgos a los que se exponen sus proyectos.

OBJETIVO DE CONTROL: AI2 Adquirir y mantener software aplicativo

Se realizó una entrevista con el gerente de operación tecnológica.

1- Se ha verificado que Medula cumpla con las legislaciones y regulaciones establecidas?

No se han realizado estas verificaciones.

2- Se ha planeado un plan para el seguimiento y mantenimiento post implementación?

Se ha comentado de manera informal las posibles acciones que se realizaran para el mantenimiento a realizar cuando el aplicativo esté funcionando.

3- Se ha comentado con los clientes la importancia de la gestión de cambios?

Si se les ha comentado la actitud para adaptarse al cambio de tecnología.

4- Se ha realizado un plan para implementación y la configuración del aplicativo Medula?

Si se ha comentado con el Hospital Pionero en obtener el aplicativo (Hospital san Onofre) pero el plan de implementación se tiene de manera informal.

5- Se realizó un plan de gestión de riesgos para verificar la seguridad de medula?

No se ha realizado

OBJETIVO DE CONTROL: AI4 FACILITAR LA OPERACIÓN Y EL USO

Se realizó una entrevista con el gerente de operación tecnológica.

1- COMPGENIOSS le brinda a los empleados manuales de usuarios, cuando estos ingresan por primera vez a la empresa?

En la empresa, no contamos con manuales de funciones, cuando ingresa un nuevo empleado, solo le informamos de forma verbal las funciones y como resolver algunos problemas que se lleguen a presentar.

2- Con que frecuencia son actualizados y documentados los manuales de usuarios y de soporte para el aplicativo MEDULA?

No contamos con ninguno de los dos manuales, así que por ende no hay actualización y documentación.

3- Los manuales de soporte del aplicativo, son desarrollados por la empresa o se requiere de terceros para la creación de estos?

Como se comentó anteriormente de momento no contamos con ninguno de los manuales pero serán realizados por personal propio de CompGenioss.

OBJETIVO DE CONTROL: AI5 Adquirir recursos de TI

Se realizó una entrevista con el gerente de operación tecnológica.

1- Se realizan capacitaciones de los empleados cuando se adquieren recursos de TI en la organización?

No se realizan capacitaciones solo se comenta a los trabajadores sobre los recursos adquiridos.

2- Que documentación se utiliza para el registro de adquisición de recursos de TI?

No se cuenta con ningún tipo de documentación.

3- Existen procesos, controles, metodologías para la selección y adquisición de recursos de TI?

Procesos definidos como tal no existe ninguno pero si se investiga a fondo las posibles opciones que brinda el mercado y de ahí se selecciona la que mejor beneficios otorgue a la organización.

4- Se requiere alguna aprobación para la adquisición de recursos de TI?

Si se requiere la aprobación del Señor Bladimir Cahuana gerente General de CompGenioss.

OBJETIVO DE CONTROL: AI6 Administrar Cambios

Se realizó una entrevista con el gerente de operación tecnológica.

1- Se encuentran establecidos procedimientos para cambios en el aplicativo?

No se encuentran establecidos procedimiento para cambios en el aplicativo

2- Se establece un proceso formal para la autorización de cambios de emergencia del aplicativo

No se tiene un proceso formal para la autorización de cambios de emergencia del aplicativo

3- Se realizan actualizaciones en el documento de manuales de usuario luego de realizar los respectivos cambios?

No se tiene documentado el manual de usuario, solo se le hacen las pruebas para probar pero no se documenta nada

OBJETIVO DE CONTROL: AI7 Instalar Y Acreditar Soluciones Y Cambios

Se realizó una entrevista con el gerente de operación tecnológica.

1- En la organización se establece un plan y un ambiente de pruebas?

No se ha establecido un plan ni ambiente de prueba; Las pruebas las realiza el desarrollador según su criterio en el momento en el que él las indique

2- Se evalúan y se aprueban los resultados de las pruebas por parte de la gerencia de la compañía?

Algunas veces se evalúan y se aprueban los resultados de las pruebas por parte de la gerencia de la compañía

3- Luego de realizar los cambio se le hace una revisión posterior a la implantación?

Si se le hace una revisión posterior a la implantación

OBJETIVO DE CONTROL: DS5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS

Se realizó una entrevista con el gerente de operación tecnológica.

1- COMPGENIOSS cuenta con un plan de seguridad de TI ?

No, no contamos con un plan de seguridad de TI, es un tema que se ha tocado en reuniones y que se piensa desarrollar en el futuro.

2- Se cuentan con políticas, metodologías y procedimientos de seguridad actualizados?

No contamos con ninguna de las tres opciones de seguridad.

3- La administración del plan de seguridad se encuentra alineado con los requerimientos del negocio?

No tenemos un plan de seguridad establecido, por ende no se encuentra alineado con el negocio.

4- Se cuenta con un repositorio central, para las identidades de usuario y los derechos de acceso?

Actualmente no contamos con ello, pero se está gestionando su implementación, así que dentro de poco, cumpliremos con este requisito de seguridad.

5- Con que frecuencia se realizan pruebas y monitoreo de seguridad, en la infraestructura tecnológica de COMPGENIOSS ?

Se realizan pruebas y monitoreo mensuales, de la infraestructura tecnológica de la empresa.

6- Se cuenta con llaves criptográficas? ¿estas, tienen implementadas políticas y procedimientos, para su uso?

No, no contamos con nada de esto.

7- Se cuenta con medidas preventivas, detectivas y correctivas en la infraestructura tecnológica de la empresa? ¿Qué tipos de medidas se utilizan?

Si se cuentan con algunas medidas de prevención, detección y corrección de la infraestructura, entre ellas el mantenimiento y monitoreo periódico de toda la tecnología de la empresa.

11.5 PRUEBAS DE LA AUDITORIA

UNIVERSIDAD DE LA COSTA

SET DE PRUEBAS

AUDITORIA AL MODULO DE CONSULTA EXTERNA DEL SISTEMA DE INFORMACIÓN MEDULA DE LA EMPRESA COMPGENIOSS LTDA.

Ingeniero: Bladimir Cahuana

Julio de 2012

SET DE PRUEBAS Auditoria al Módulo de Consulta Externa del Aplicativo MEDULA			
Fecha:	10 de Junio 2012	**Prueba N°:**	01
Tipo de Prueba:			
Control a Evaluar:	1. Adecuada parametrización de los campos del aplicativo		
1. Nombre de la Prueba:			
➢ Prueba de estandarización de usuarios y claves.			
2. Objetivo:			
➢ Verificar que tipo de estructura o estándar se tiene en cuenta al momento de hacer la creación del login del usuario			
3. Descripción de la Prueba:			
1. Se solicita el listado de los usuarios registrados en el sistema o la matriz de roles y perfiles 2. Se procede a realizar una revisión de los mismos. 3. Se verifica que tipo de estructura o estándar se tiene en cuenta al momento de asignarle un login al usuario.			

SET DE PRUEBAS Auditoria al Módulo de Consulta Externa del Aplicativo MEDULA			
Fecha:	10 de Junio 2012	**Prueba N°:**	02
Tipo de Prueba:			
Control a Evaluar:	2. Existencia de Políticas para la Protección y seguridad de los Datos		

1. Nombre de la Prueba:

- Prueba de acceso a la Base de Datos.

2. Objetivo:

- Verificar la existencia de un login único, que permita el acceso a la base de datos de MEDULA, por parte del DBA.

3. Descripción de la Prueba:

1. Se solicitan, los registros de los Logs, de los ingresos realizados por el DBA en el sistema.

2. Se procede a realizar una revisión de los mismos.

3. Se realiza un filtro en el campo "usuario" y "password", para ver solo los usuarios y las respectivas claves con las cuales se acceden a la base de datos.

SET DE PRUEBAS Auditoria al Módulo de Consulta Externa del Aplicativo MEDULA			
Fecha:	10 de Junio 2012	**Prueba N°:**	03
Tipo de Prueba:			
Control a Evaluar:	3. Adecuada definición de políticas de roles y perfiles para el acceso a la base de datos.		

1. Nombre de la Prueba:

- Prueba de Roles y Perfiles

2. Objetivo:

- Verificar los diferente Roles y Perfiles de usuarios, creados y con acceso en la base de datos.

3. Descripción de la Prueba:

1. Se solicita al DBA, la matriz de Roles y Perfiles, de la base de datos.
2. Si el DBA, no cuenta con una matriz de Roles y Perfiles, se procede a solicitarle un registro de los logs de usuarios creados y que tienen acceso a la base de datos.
3. Se procede a verificar la información suministrada.
4. Se realiza un filtro en los campo "usuario", "Perfil", "Privilegios", para ver solo los usuarios y los respectivos perfiles y privilegios, que estos tienen asignados en la base de datos.

4. Resultado de la Prueba:

Luego de haber realizado las pruebas, se identificó, que existen dos (2) usuarios, (ALCIDES y ACARMONA), con perfil de administrador con privilegios de creación de usuarios y modificación y eliminación, además existe un tercer usuario (JREDONDO), con perfil NORMAL, con privilegios de consulta e ingreso de datos en el sistema.

SET DE PRUEBAS Auditoria al Módulo de Consulta Externa del Aplicativo MEDULA			
Fecha:	10 de Junio 2012	**Prueba N°:**	04
Tipo de Prueba:	Funcional		
Control a Evaluar:	4. Existencia de controles y validación de acceso al sistema		

1. Nombre de la Prueba:

- Prueba de Intentos Fallidos

2. Objetivo:

- Con esta prueba se pretende establecer cuál es el número de intentos fallidos permitidos, para ingresar al sistema.

3. Descripción de la Prueba:

1. Se abre el aplicativo.
2. En la casilla de usuario, se digita un usuario que se encuentre creado en el sistema.
3. En la casilla de contraseña, se digita una clave errónea, que no corresponda, con la del usuario escogido.
4. Se repite el paso anterior X cantidad de veces, hasta que el sistema arroje una acción, que impida seguir con los intentos.

4. Resultado de la Prueba:

Luego de realizar la prueba a cabalidad, se observo que después de ingresar dos (2) veces claves de acceso al sistema de forma errónea, el sistema arrojó un mensaje de "Demasiados intentos con claves erróneas". Con lo cual se permite establecer que el número de ingresos permitidos que tiene el usuario para ingresar al sistema, consta solo de dos intentos.

SET DE PRUEBAS Auditoria al Módulo de Consulta Externa del Aplicativo MEDULA			
Fecha:	10 de Junio 2012	**Prueba N°:**	05
Tipo de Prueba:	Funcional		
Control a Evaluar:	4. Existencia de controles y validación de acceso al sistema		

1. Nombre de la Prueba:

- Prueba de Longitud de Clave

2. Objetivo:

- Con esta prueba se pretende establecer cuál es la longitud total permitida, al momento de ingresar la clave de acceso al sistema.

3. Descripción de la Prueba:

1. Se ingresa al aplicativo, por medio del usuario administrador, el cual es el único que tiene el permiso de creación de usuario.
2. Se escoge la opción en el sistema de creación de nuevo usuario y clave.
3. Se procede a crear un nombre de usuario.
4. En la opción de Contraseña, se ingresan números consecutivos, que van desde el numero 1 hasta el numero límite permitido.

4. Resultado de la Prueba:

Luego de realizar la prueba, se evidencio que la longitud mínima permitida para ingresar la clave de acceso al sistema es de un (1) digito alfanumérico y la longitud máxima permitida es de siete dígitos alfanuméricos (7).

SET DE PRUEBAS Auditoria al Módulo de Consulta Externa del Aplicativo MEDULA			
Fecha:	10 de Junio 2012	**Prueba N°:**	06
Tipo de Prueba:	Funcional		
Control a Evaluar:	5. Existencia de políticas y procedimientos para la administración de la BD		
1. Nombre de la Prueba:			
➢ Prueba de la existencia de un solo administrador			
2. Objetivo:			
➢ Verificar la existencia de un único usuario con perfil de administrador.			
3. Descripción de la Prueba:			
1. Se solicita el listado de los usuarios registrados en el sistema o la matriz de roles y perfiles. 2. Se procede a realizar una revisión de los mismos. 3. Se realiza un filtro en campo perfil para verificar si existe un único usuario administrador			
4. Resultado de la Prueba:			
Luego de realizar las pruebas respectivas, se evidencio que existen dos (2) usuarios con perfil de administrador del sistema, (ALCIDES y ACARMONA), pero con claves de acceso diferentes.			

SET DE PRUEBAS Auditoria al Módulo de Consulta Externa del Aplicativo MEDULA			
Fecha:	10 de Junio 2012	**Prueba N°:**	07
Tipo de Prueba:	Funcional		
Control a Evaluar:	6. Existencia de procedimientos y documentación de los cambios que se realicen en la base de datos		

1. Nombre de la Prueba:

- Prueba de Cambios en la base de datos.

2. Objetivo:

- Verificar la existencia de procedimientos y cambios que se hallan realizado en la base de datos.

3. Descripción de la Prueba:

1. Se solicitan, los registros de los Logs, de las acciones ejecutadas por el DBA en el sistema.

2. Se procede a realizar una revisión de los mismos.

3. Se realiza un filtro en el campo "evento", para ver solo las acciones y cambios realizadas por el DBA en el sistema.

SET DE PRUEBAS Auditoria al Módulo de Consulta Externa del Aplicativo MEDULA			
Fecha:	10 de Junio 2012	**Prueba N°:**	08
Tipo de Prueba:	Funcional		
Control a Evaluar:	7. Adecuada integridad y consistencia de la base de datos		

1. Nombre de la Prueba:

- Prueba de Creación en la Base de Datos.

2. Objetivo:

- Verificar si los datos y perfiles que se crean, por medio de la interfaz del aplicativo MEDULA, son almacenados correctamente en la Base de Datos.

3. Descripción de la Prueba:

1. Se ingresa al aplicativo con un usuario registrado del sistema.
2. Se escoge el / los formularios del aplicativo en el cual se desea crear el perfil de datos, por medio de la interfaz.
3. Se ingresa la información solicitada en el formulario, este paso se realiza las veces que se deseen.
4. Se solicita al DBA un registro de la información ingresada anteriormente y almacenada en la base de datos.
5. Se verifica si la información se ingresó correctamente o no, al sistema.

SET DE PRUEBAS Auditoria al Módulo de Consulta Externa del Aplicativo MEDULA			
Fecha:	10 de Junio 2012	**Prueba N°:**	09
Tipo de Prueba:	Funcional		
Control a Evaluar:	7. Adecuada integridad y consistencia de la base de datos		

1. Nombre de la Prueba:

- Prueba de Inserción en la Base de Datos.

2. Objetivo:

- Verificar si los datos que se ingresan, por medio de la interfaz del aplicativo MEDULA, son almacenados correctamente en la Base de Datos.

3. Descripción de la Prueba:

1. Se ingresa al aplicativo con un usuario registrado del sistema.
2. Se escoge el / los formularios del aplicativo al cual se desea ingresar la información, por medio de la interfaz.
3. Se ingresa la información solicitada en el formulario, este paso se realiza las veces que se deseen.
4. Se solicita al DBA un registro de la información ingresada anteriormente y almacenada en la base de datos.
5. Se verifica si la información se ingresó correctamente o no, al sistema.

4. Resultado de la Prueba:

Luego de realizar la prueba a cabalidad, se evidencio que la información ingresada al sistema por medio de la interfaz de usuario, es almacenada de forma correcta en la base de datos, con un debido orden de los datos.

SET DE PRUEBAS Auditoria al Módulo de Consulta Externa del Aplicativo MEDULA			
Fecha:	10 de Junio 2012	**Prueba N°:**	10
Tipo de Prueba:	Funcional		
Control a Evaluar:	7. Adecuada integridad y consistencia de la base de datos		

1. Nombre de la Prueba:

- Prueba de Eliminación en la Base de Datos.

2. Objetivo:

- Verificar si los datos que se eliminan, por medio de la interfaz del aplicativo MEDULA, son eliminados correctamente también en la Base de Datos.

3. Descripción de la Prueba:

1. Se ingresa al aplicativo con un usuario registrado del sistema.
2. Se escoge el / los formularios del aplicativo en el cual se desea eliminar la información almacenada en estos, por medio de la interfaz.
3. Se realiza la eliminación de la información escogida.
4. Se solicita al DBA un registro actualizado de la información almacenada en la base de datos de el / los formularios seleccionados anteriormente.
5. Se verifica en los registros si la información solicitada fue eliminada correctamente de la base de datos.

4. Resultado de la Prueba:

Luego de realizar la prueba a cabalidad, se evidencio que la información eliminada en el sistema por medio de la interfaz de usuario, también fue eliminada de forma correcta de la base de datos.

SET DE PRUEBAS Auditoria al Módulo de Consulta Externa del Aplicativo MEDULA			
Fecha:	10 de Junio 2012	**Prueba N°:**	11
Tipo de Prueba:	Funcional		
Control a Evaluar:	8. Existencia de Documentación actualizada del sistema (Incluye manuales técnicos- usuario - instalación)		

1. Nombre de la Prueba:

- Prueba de Manuales.

2. Objetivo:

- Verificar si la información contenida en los manuales de usuarios y soporte, corresponden con la versión del aplicativo y si estos permiten solucionar problemas que se puedan presentar en el aplicativo y a los usuarios en su manejo.

3. Descripción de la Prueba:

1. Se solicita al gerente de COMPGENIOSS, los manuales de usuario y de soporte del aplicativo.

2. Si se cuenta con los manuales, se avanza al siguiente paso, sino se tienen los manuales se finaliza la prueba.

3. Se verifica si la versión de los manuales corresponde con la versión del aplicativo.

4. Se toman un grupo de pasos y tareas al azar de los manuales y se ejecutan en el aplicativo, para verificar el correcto funcionamiento de los manuales tanto de usuarios como de soporte.

SET DE PRUEBAS Auditoria al Módulo de Consulta Externa del Aplicativo MEDULA			
Fecha:	10 de Junio 2012	**Prueba N°:**	12
Tipo de Prueba:	Funcional		
Control a Evaluar:	9. Documentación de los requerimientos funcionales del sistema.		

1. Nombre de la Prueba:

- Prueba de Funcionalidad del Sistema

2. Objetivo:

- Verificar si la funcionalidad del sistema, cumple con los requerimientos establecidos.

3. Descripción de la Prueba:

1. Se solicita al gerente de COMPGENIOSS, la lista de los requerimientos funcionales del sistema.
2. Se toman un grupo de requerimientos al azar.
3. Se ejecutan en el aplicativo.
4. Se verifica el correcto funcionamiento del sistema, de acuerdo a los requerimientos establecidos.

SET DE PRUEBAS Auditoria al Módulo de Consulta Externa del Aplicativo MEDULA			
Fecha:	10 de Junio 2012	**Prueba N°:**	13
Tipo de Prueba:	Funcional		
Control a Evaluar:	18. Existencia de copias de respaldo (Backup).		

1. Nombre de la Prueba:

- Prueba de Backup

2. Objetivo:

- Evaluar si el sistema cuenta con opción, para realizar copias de respaldo.

3. Descripción de la Prueba:

1. Ingresar al sistema, por medio de un usuario registrado.
2. Identificar si el sistema cuenta, con opción de Copias de Respaldo. Si lo tiene, se avanza al siguiente paso, sino se finaliza la prueba.
3. Se escoge las fechas entre las cuales se requiera realizar las copias de la información y se procede a guardar la copia.
4. Ejecutar la copia y verificar si la información del Backup, corresponde a la información original almacenada en el sistema.

SET DE PRUEBAS Auditoria al Módulo de Consulta Externa del Aplicativo MEDULA			
Fecha:	10 de Junio 2012	**Prueba N°:**	14
Tipo de Prueba:	Funcional		
Control a Evaluar:	19. Existencia de una bitácora de fallas para identificar problemas que presente el aplicativo		

1. Nombre de la Prueba:

- Prueba de Estabilidad del Aplicativo

2. Objetivo:

- Evaluar la capacidad que tiene el sistema para responder a fallas y errores.

3. Descripción de la Prueba:

1. Ingresar al sistema, por medio de un usuario registrado.
2. Realizar el número mayor de acciones sobre el sistema, en el menor tiempo, para hacer que este falle intencionalmente.
3. Contabilizar el tiempo que tarda el sistema en recuperarse después de las fallas a las cuales fue sometida.
4. Verificar si el sistema funciona correctamente o si sigue presentando fallas.

UNIVERSIDAD DE LA COSTA

ALINEACION DE MARCOS DE REFERENCIA

AUDITORIA AL MODULO DE CONSULTA EXTERNA DEL SISTEMA DE INFORMACIÓN MEDULA DE LA EMPRESA COMPGENIOSS LTDA.

Ingeniero: Bladimir Cahuana
Julio de 2012

OBJETIVOS DE CONTROL COBIT SELECCIONADOS PARA EL DESARROLLO DE LA AUDITORIA

PO3 - DETERMINAR LA DIRECCIÓN TECNOLOGICA

- PO3.3 Monitoreo de Tendencias y Regulaciones Futuras

PO9 - EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI

- PO 9.3 Identificación de eventos
- PO 9.4 Evaluación de riesgos de TI
- PO 9.5 Respuesta a los riesgos
- PO 9.6 Mantenimiento y monitoreo de un plan de acción de riesgos

PO10 - ADMINISTRAR PROYECTOS

- PO 10.2 Marco de trabajo para la administración de proyectos
- PO 10.5 Declaración del alcance del proyecto
- PO 10.8 Recursos del proyecto
- PO 10.9 Administración de riesgos del proyecto
- PO 10.11 Control de cambios del proyecto

AI2 - ADQUIRIR Y MANTENER SOFTWARE APLICATIVO

- AI 2.3 Control y posibilidad de auditar las aplicaciones
- AI 2.4 Seguridad y disponibilidad de las aplicaciones
- AI 2.10 Mantenimiento de software aplicativo

AI4 – FACILITAR LA OPERACIÓN Y EL USO

- AI 4.3 Transferencia de conocimiento a usuarios finales
- AI 4.4 Transferencia de conocimiento a personal de operaciones y soporte

AI5 - ADQUIRIR RECURSOS DE TI

- AI 5.1 Control de adquisición
- AI 5.4 Adquisición de recursos de TI

DS5 – GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS

- DS 5.3 Administración de identidad
- DS 5.4 Administración de cuentas de usuario

RELACION OBJETIVOS DE CONTROL COBIT CON ITIL V3 E ISO 27002

PO3 - DETERMINAR LA DIRECCIÓN TECNOLOGICA

PO3.3 MONITOREO DE TENDENCIAS Y REGULACIONES FUTURAS

Relación con otros estándares:

ITIL V3:

- 4.5.5.4 Supervisión del régimen de la identidad

ISO 27002:

- 15.1.1 Identificación de la legislación aplicable.
- 15.1.2 Derechos de propiedad intelectual (DPI).
- 15.1.3 Protección de los documentos de la organización.
- 15.1.4 Protección de datos y privacidad de la información de carácter
- personal.
- 15.1.5 Prevención del uso indebido de recursos de tratamiento de la
- información.
- 15.1.6 Regulación de los controles criptográficos.
- 15.2.1 Cumplimiento de las políticas y normas de seguridad.

Las buenas prácticas sugieren:

COBIT 4.1: Sugiere establecer procesos para monitorear las tendencias tecnológicas, infraestructuras, legales y regulatorias. Incluir las consecuencias de estas tendencias en el desarrollo del plan de infraestructura tecnológica de TI.

ISO 27002: Sugiere que los directivos deberían asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente y cumplen con los estándares y políticas de seguridad.

PO9 - EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI

PO9.3 IDENTIFICACIÓN DE EVENTOS

Relación con otros estándares:

ITIL V3:

- SS 9.5 Riesgos
- SD 4.5.5.2 Requisitos y estrategia

ISO 27002:

- 13.1.1 Reporte de eventos de seguridad de información
- 13.1.2 Reporte de debilidades de seguridad

Las buenas prácticas sugieren:

COBIT 4.1: Sugiere identificar eventos tales como amenazas que puedan explotar una vulnerabilidad existente y que causaría un impacto potencial y negativo sobre los objetivos del negocio y nos sugiere determinar la amenaza del impacto y mantener esta información documentada.

ITIL V3: Nos indica que el principal factor de riesgo en una organización es la falta de información precisa, es decir, que si se detecta un riesgo o amenaza y no es informada y comunicada a tiempo para su gestión tiende a materializarse por este motivo nos invita a la creación de estrategias para el tratamiento de eventos no deseados.

ISO 27002: Complementa este control si empleados, contratistas y terceros comunican cualquier debilidad observada a la mayor brevedad posible mediante canales de gestión apropiados

PO 9.4 EVALUACIÓN DE RIESGOS DE TI

Relación con otros estándares:

- **ITIL V3:**
- SS 9.5 Riesgos
- D 4.5.5.2 Requisitos y estrategia
- SD 8.1 Análisis de impacto en el negocio
- ST 4.6 Evaluación

ISO 27002:

- Revisión de la política de seguridad de la información
- 14.1.2 Continuidad del negocio y evaluación de riesgos

Las buenas prácticas sugieren:

COBIT 4.1: Sugiere que debe evaluarse de forma recurrente la probabilidad como el impacto de los riesgos ya identificados por medio de métodos cualitativos y cuantitativos.

ITIL V3: Sugiere realizar una evaluación precisa de los riesgos analizando la consecuencia probabilidad y oportunidades de mejoras que puedan presentarse, también indica que se debe contar con planes de continuidad del negocio y recuperación de desastres.

ISO 27002: Sugiere que la política de seguridad de información debe ser revisada en intervalos planificados o en casos especiales para garantizar su eficiencia y se deben identificar eventos causantes de interrupciones a los procesos así como la probabilidad e impacto de dichas interrupciones.

PO9.5 RESPUESTA A LOS RIESGOS

Relación con otros estándares:

ITIL V3:

- SS 9.5 Riesgos
- SD 4.5.5.3 Implementación
- ST 4.6 Evaluación

Las buenas prácticas sugieren:

COBIT 4.1: Sugiere la creación de procesos de respuesta a riesgos para validar controles efectivos en beneficios y costos de manera constante en estos procesos se deben tener claramente definidos las medidas que se deben tomar para con los riesgos ya sea evitarlo, mitigarlo, aceptarlo y/o compartirlo.

ITIL V3: Sugiere un tratamiento de riesgos en los cuales se contemplen diversas opciones con el fin de disminuir el impacto y su probabilidad para este los riesgos deben estar claramente identificados y valorados para luego proceder a un tratamiento de reducción a tal manera de impedir su materialización.

PO9.6 MANTENIMIENTO Y MONITOREO DE UN PLAN DE ACCIÓN DE RIESGOS

Relación con otros estándares:

ITIL V3:

- SS 9.5 Riesgos
- SD 4.5.5.4 Operación continúa

Las buenas prácticas sugieren:

COBIT 4.1: Sugiere una planificación de las actividades de control para todos los niveles con el fin de implementar la respuesta a los riesgos, en las cuales deben estar claramente identificados el costo/beneficio y responsable de la ejecución del control, debe de monitorearse la ejecución de los planes de riesgos y en caso de una emergencia debe de informarse a la alta gerencia.

ITIL V3: Sugiere el monitoreo continuo a los planes de prevención de riesgos con el fin de asegurar y garantizar que se actuara de forma correcta en caso de un incidente que pueda impedir o retrasar los procesos de TI.

PO10 - ADMINISTRAR PROYECTOS

PO10.2 MARCO DE TRABAJO PARA LA GESTIÓN DE PROYECTOS

Relación con otros estándares:

No se encontró relación con ITIL V3 e ISO 27002

Las buenas prácticas sugieren:

COBIT 4.1: Sugiere que se debe establecer y mantener un marco de trabajo para la administración de los proyectos en el cual debe encontrarse definido todo lo relacionado al alcance, limite y metodologías de los proyectos.

PO10.5 DECLARACIÓN DE ALCANCE DEL PROYECTO

Relación con otros estándares:

ITIL V3:

- SD 3.4 Identificar y documentar los requerimientos y drivers del negocio
- SD 3.5 Actividades de diseño

Las buenas prácticas sugieren:

COBIT 4.1: Sugiere la definición, creación y documentación de un alcance del proyecto que se desea desarrollar con el fin de crear un entendimiento común sobre el alcance del

proyecto las partes interesadas, antes de iniciarse el proyecto el alcance debe estar aprobado por los patrocinadores y favorecedores.

ITIL V3: Sugiere que se debe conservar una información precisa, clara y concisa, sencilla y pertinente sobre los requerimientos del negocio y sus conductos, para proporcionar un catálogo apropiado de los servicios que se ajustan a las necesidades de la empresa, para que de esta manera haya un entendimiento común de los requerimientos del negocio, esta información es muy importante para el diseño y entrega de nuevos servicios o cambios en los existentes. Esta información debe ser acordada con los representantes de la empresa.

PO10.8 RECURSOS DEL PROYECTO

Relación con otros estándares:

No se encontró relación con ITIL V3 e ISO 27002

Las buenas prácticas sugieren:

COBIT 4.1: sugiere que, se deben definir las responsabilidades, relaciones, autoridades y criterios de desempeño de cada uno de los miembros del equipo, para de esta manera poder asignarlos correctamente a cada miembro del equipo y de esta manera alcanzar los objetivos planteados, todo esto usando las prácticas de adquisición de la organización.

PO10.9 GESTIÓN DE RIESGOS DEL PROYECTO

Relación con otros estándares:

No se encontró relación con ITIL V3 e ISO 27002

Las buenas prácticas sugieren:

COBIT 4.1: sugiere que, se deben elimina o minimizar los riesgos que estén asociados a los proyectos individuales, por medio de diversos procesos a las áreas o eventos que pueden generar cambios no deseados. Los riesgos que se presente a consecuencia del proceso y el producto resultante del proyecto se deben establecer y registrar de forma central.

PO10.11 CONTROL DE CAMBIOS DEL PROYECTO

Relación con otros estándares:

ITIL V3:

- ST 3.2.10 Anticipar y gestionar correcciones de curso

Las buenas prácticas sugieren:

COBIT 4.1: sugiere que, se deben establecer sistemas de control de cambios en cada proyecto, de tal manera todos estos cambios se puedan revisar, aprobar e incorporar al plan integrado del proyecto, todo esto bajo el marco de trabajo de gobierno del programa y del proyecto.

ITIL V3: sugiere que se debe capacitar al personal, para que estos sean capaces de reconocer los cambios o variaciones en el proyecto, para que de esta manera se puedan tomar correcciones en el rumbo del proyecto. Proporcionar información sobre los cambios que se aplicaron después de la configuración línea de base fue establecida.

AI2 - ADQUIRIR Y MANTENER SOFTWARE APLICATIVO

AI2.3 CONTROL Y AUDITABILIDAD DE LAS APLICACIONES

Relación con otros estándares:

ISO 27002:

- 10.10.1 registro de auditoría
- 10.10.5 registro de fallas
- 12.2.1 Validación de datos de entrada
- 12.2.2 Control de procesamiento interno
- 12.2.3 Integridad de mensajes
- 12.2.4 Validación de datos de salida
- 13.2.3 Recolección de evidencia
- 15.3.1 Controles de auditoría de sistemas de información
- 15.3.2 Protección de herramientas de auditoría de sistemas de información

Las buenas prácticas sugieren:

COBIT 4.1: sugiere que, se deben implementar controles de negocios, cuando sea necesario a controles de aplicación automatizados, de tal modo que el proceso sea exacto, completo, oportuno, autorizado y auditable

Iso 27002: sugiere que se debe crear y mantener por periodos de tiempo definidos los registros o logs de auditoria generado por los usuarios, excepciones y eventos de

seguridad de la información esto se debe hacer con el propósito de investigaciones en un futuro y monitoreo de controles de acceso.

AI2.4 SEGURIDAD Y DISPONIBILIDAD DE LAS APLICACIONES

Relación con otros estándares:

ITIL V3:

- SD 3.6.1 Diseño de soluciones de servicios
- SO 4.4.5.11 Errores detectados en el entorno de desarrollo

ISO 27002:

- 6.1.4 Proceso de autorización para las instalaciones de procesamiento de información
- 7.2.1 Lineamientos para la clasificación
- 10.3.2 Aceptación del sistema
- 11.6.2 Aislamiento de sistemas sensitivos
- 12.1.1 Análisis y especificación de los requisitos de seguridad
- 12.2.3 Integridad de mensajes
- 12.3.1 Política de uso de controles criptográficos
- 12.4.3 Control de acceso al código fuente de los programas
- 12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo
- 12.5.4 Fuga de información
- 15.3.2 Protección de herramientas de auditoría de sistemas de información

Las buenas prácticas sugieren:

COBIT 4.1: sugiere que, se deben abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad, como respuesta a los riesgos que se encuentran identificados, todo esto en dirección con la clasificación de los datos, la arquitectura de la información y la tolerancia a riesgos de la organización.

ITIL V3: Sugiere que, debe existir una transferencia de conocimientos en todas las etapas entre el personal operativo y el personal del proyecto, para garantizar la seguridad del negocio, debido a que las nuevas aplicaciones, sistemas o actualizaciones de software estén completamente libre de errores.

Iso 27002: sugiere que se deben definir criterio para la aceptación de los sistemas de informaciones que se adquieren luego se deben realizar las pruebas pertinentes con el fin de garantizar que el sistema será estable, seguro y se pueda avalar su disponibilidad.

AI2.10 MANTENIMIENTO DEL SOFTWARE APLICATIVO

Relación con otros estándares:

No se encontró relación con ITIL V3 e ISO 27002

Las buenas prácticas sugieren:

COBIT 4.1: sugiere que, se debe desarrollar una estrategia y plan para el mantenimiento de las aplicaciones de software.

AI4 – FACILITAR LA OPERACIÓN Y EL USO

AI4.3 TRANSFERENCIA DE CONOCIMIENTO A USUARIOS FINALES

Relación con otros estándares:

ITIL V3:

- Proporcionar sistemas para la transferencia de conocimiento y apoyo a las decisiones.

Las buenas prácticas sugieren:

COBIT 4.1: Sugiere que se transfieran los conocimientos y las habilidades, para permitir que los usuarios finales utilicen con efectividad y eficiencia el sistema de aplicación, como apoyo a los procesos del negocio. La transferencia del conocimiento incluye el desarrollo de un plan de entrenamiento inicial y continuo, así como el desarrollo de habilidades, material de entrenamiento, manuales de usuario, manuales de procedimiento, ayuda en línea, asistencia a usuarios, identificación del usuario clave y evaluación.

ITIL v3. Sugiere proporcionar herramientas de fácil acceso, presentación y elaboración de informes, además de ofrecer interfaces de usuario y herramientas de calidad para diferentes personas y roles para tomar decisiones en los momentos oportunos. Resumir y publicar los efectos previstos del cambio e imprevisto, precisa activar las transacciones de aprobación y notificación para la toma de decisiones a través de herramientas de flujo de trabajo.

AI4.4 TRANSFERENCIA DE CONOCIMIENTO A PERSONAL DE OPERACIONES Y SOPORTE

Relación con otros estándares:

ITIL V3:

- Proporcionar sistemas para la transferencia de conocimiento y apoyo a las decisiones.

Las buenas prácticas sugieren:

COBIT 4.1: sugiere que se transfiera el conocimiento y las habilidades, para permitir al personal de soporte técnico y de operaciones, entregar, apoyar y mantener la aplicación y la infraestructura asociada de manera efectiva y eficiente, de acuerdo a los niveles de servicios requeridos. La transferencia del conocimiento debe incluir un entrenamiento inicial y continuo, el desarrollo de las habilidades, los materiales de entrenamientos, los manuales de operación, los manuales de procedimientos y escenarios de atención al usuario.

ITIL v3. Sugiere proporcionar herramientas de fácil acceso, presentación y elaboración de informes, además de ofrecer interfaces de usuario y herramientas de calidad para diferentes personas y roles para tomar decisiones en los momentos oportunos. Resumir y publicar los efectos previstos del cambio e imprevisto, precisa activar las transacciones de aprobación y notificación para la toma de decisiones a través de herramientas de flujo de trabajo.

AI5 - ADQUIRIR RECURSOS DE TI

AI5.1 CONTROL DE ADQUISICIONES

Relación con otros estándares:

ITIL V3:

- SD 3.7.2 Adquisición de la solución elegida

ISO 27002:

- 6.1.5 Acuerdos de confidencialidad

Las buenas prácticas sugieren:

COBIT 4.1: sugiere que, se debe desarrollar y seguir una serie de procedimientos y estándares fundamentados en, el proceso general y la estrategia general de adquisición de la organización, para de esta manera, poder adquirir una infraestructura que esté relacionada con TI, instalaciones de hardware y servicios necesarios para el negocio.

ISO 27002: sugiere que se deben revisar regularmente los acuerdos de confidencialidad, con el fin de proteger la información importante de la organización, para así garantizar la protección de los intereses del proyecto.

AI5.4 ADQUISICIÓN DE RECURSOS TI

Relación con otros estándares:

ITIL V3:

- SD 3.7.2 Adquisición de la Solución elegida.

Las buenas prácticas sugieren:

COBIT 4.1: sugiere que, se debe proteger y cumplir los intereses de la organización en todos los contratos de adquisiciones, abarcando los derechos y obligaciones de las partes en los términos pactados para la adquisición de software, recursos de desarrollo, infraestructura y servicios.

ITIL V3: sugiere que, cuando se necesiten los proveedores del software para la solución de problemas, se deben seguir ciertas etapas para proteger los intereses del proyecto, como son, la finalización de los controles necesarios en el proveedor y la finalización de los términos y condiciones de nuevos contratos, asegurándose que se apliquen las políticas de la empresa.

AI6 – ADMINISTRAR CAMBIOS

AI6.1 ESTANDARES Y PROCEDIMIENTOS PARA CAMBIOS

Relación con otros estándares:

ITIL V3:

- SD 3.2 Diseño balanceado
- SD 3.7 Actividades subsiguientes del diseño
- ST 3.2 Políticas para la transición del servicio
- ST 3.2.1 Definir e implementar una política formal para la transición del servicio
- ST 3.2.2 Implementar todos los cambios a los servicios a través de la transición del servicio
- ST 3.2.7 Establecer controles y disciplinas eficaces
- ST 4.1 Planificación y soporte para la transición
- ST 4.1.4 Políticas, principios y conceptos básicos
- ST 4.2 Gestión de cambios

ISO 27002:

- 10.1.2 Gestión de cambios
- 12.5.3 Restricciones en los cambios a los paquetes de software

Las buenas prácticas sugieren:

COBIT 4.1: Sugiere establecer procedimientos de administración de cambios formales para manejar de manera estándar todas las solicitudes para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio y las plataformas fundamentales.

ITIL V3: Sugiere que, en el proceso de cambio, si éste se lleva a cabo, se haga de la forma más eficiente, siguiendo los procedimientos establecidos y asegurando en todo momento la calidad y continuidad del servicio TI.

ISO 27002: Sugiere que los sistemas operacionales y el software de aplicación deben ser sujetos a un estricto control de la gestión de cambios. El control inadecuado de los cambios a los sistemas y recursos de procesamiento de información es una causa común de fallas del sistema o de seguridad. Cambios en el ambiente operacional, especialmente cuando se transfiere un sistema de la etapa de desarrollo a la de operación, pueden impactar en la fidelidad de las aplicaciones

AI6.3 CAMBIOS DE EMERGENCIA

Relación con otros estándares:

ITIL V3:

- ST 4.2.6.9 Cambios de emergencia

ISO 27002:

- 10.1.2 Gestión de cambios
- 11.5.4 Uso de utilitarios del sistema
- 12.5.1 Procedimiento de control de cambios
- 12.5.3 Restricciones en los cambios a los paquetes de software
- 12.6.1 Control de vulnerabilidades técnicas

Las buenas prácticas sugieren:

COBIT 4.1: Se basa en establecer un proceso para: Definir, Plantear, Evaluar y Autorizar los cambios de emergencia que no sigan el proceso establecido, así como también conocer las pruebas una vez se hayan implementado los cambios de emergencia.

ITIL V3: Sugiere que aunque habitualmente los cambios realizados mediante procedimientos de emergencia son resultado de una planificación deficiente a veces resultan inevitables. Es esencial que al cierre del cambio de emergencia se disponga de la misma información de la que dispondríamos tras un cambio normal. Si esto no fuera así se podrían provocar situaciones de cambios futuros incompatibles, configuraciones registradas incorrectas, etc. que serían fuente de nuevas incidencias y problemas.

ISO 27002: Sugiere que los cambios a los sistemas operacionales deben realizarse solamente cuando existe una razón de negocio valida, como un incremento en el riesgo al sistema.

AI6.4 SEGUIMIENTO Y REPORTE DEL ESTATUS DE CAMBIO

Relación con otros estándares:

ITIL V3:

- ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado
- ST 3.2.14 Mejora proactiva de la calidad durante la transición del servicio
- ST 4.1.5.3 Planificar y coordinar la transición del servicio
- ST 4.1.6 Brindar soporte

ISO 27002:

- 10.1.2 Gestión de cambios

Las buenas prácticas sugieren:

COBIT 4.1: Se basa en establecer un sistema de seguimiento de mantener actualizados a los solicitantes de cambio y los interesados relevantes, acerca del estatus del cambio. Dicho estatus debe estar enfocado en los siguientes aspectos: Aplicaciones, procedimientos, procesos de parámetros del sistema y del servicio, plataformas fundamentales

ITIL V3: Sugiere que los clientes y proveedores no deben percibir el cambio como algo inesperado. Es función de la Gestión de Cambios mantener informados a los usuarios de los futuros cambios y, dentro de lo posible, hacerles participes del mismo

ISO 27002: Sugiere que los sistemas operacionales y el software de aplicación deben ser sujetos a un estricto control de la gestión de cambios. En particular se deberían considerar los siguientes controles y medidas: a) la identificación y registro de cambios significativos; b) planeamiento y prueba de los cambios; c) la evaluación de los posibles impactos, incluyendo impactos de seguridad, de dichos cambios; d) un procedimiento formal de aprobación de los cambios propuestos; e) la comunicación de los detalles de cambio a todas las personas que corresponda; f) procedimientos que identifiquen las responsabilidades de abortar y recobrarse de los cambios sin éxito y de acontecimientos imprevistos.

AI6.5 CIERRE Y DOCUMENTACIÓN DEL CAMBIO

Relación con otros estándares:

ITIL V3:

- ST 4.2.6.4 Valorar y evaluar el cambio
- ST 4.2.6.7 Revisar y cerrar el registro del cambio
- ST 4.4.5.10 Revisar y cerrar la transición del servicio
- ST 4.4.5.9 Revisar y cerrar un despliegue
- SO 4.3.5.5 Cierre

ISO 27002:

- 10.1.2 Gestión de cambios

Las buenas prácticas sugieren:

COBIT 4.1: Se enmarca en actualizar los cambios que se hacen al sistema asociado y la documentación del usuario y procedimientos correspondientes, así como también hacer un proceso de revisión para garantizar la implantación completa de los cambios.

ITIL V3: Sugiere que antes de proceder al cierre del cambio es necesario realizar una evaluación que permita valorar realmente el impacto del mismo en la calidad del servicio y en la productividad de la organización

ISO 27002: Sugiere Asegurar que todos los cambios sea evaluados, aprobados, implementados y revisados de una manera controlada

AI7 – INSTALAR Y ACREDITAR SOLUCIONES Y CAMBIOS

AI7.2 PLAN DE PRUEBA

Relación con otros estándares:

ITIL V3:

- ST 4.5.5.1 Gestión de pruebas y validación
- ST 4.5.5.2 Planificar y diseñar pruebas
- ST 4.5.5.3 Verificar el plan y el diseño de pruebas
- ST 4.5.5.4 Preparar el entorno de pruebas

ISO 27002:

- 12.5.1 Procedimientos de control de cambios
- 12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo

Las buenas prácticas sugieren:

COBIT 4.1: Sugiere establecer un plan basado en estándares de la organización que define roles, responsabilidades y criterios de entrada y salida

ITIL V3: Sugiere que las pruebas no deben limitarse a una validación de carácter técnico (ausencia de errores) sino que también deben realizarse pruebas funcionales con usuarios reales para asegurarse de que la versión cumple los requisitos establecidos y es razonablemente usable (siempre existe una inevitable resistencia al cambio en los

usuarios que debe ser tenida en consideración). Cuanto mayor sea el alcance del plan de pruebas, mayores serán las garantías de fiabilidad de la nueva versión.

ISO 27002: Sugiere revisar técnicas de aplicaciones tras efectuar cambios en el sistema operativo y también restricciones a los cambios en los paquetes de software. No se tiene que permitir la fuga ni la filtración de información no requerida.

AI7.3 PLAN DE IMPLANTACIÓN

Relación con otros estándares:

ITIL V3:

- ST 3.2.9 Planificar la liberación y el despliegue de paquetes
- ST 4.1.5.2 Preparación para la transición del servicio
- ST 4.4.5.2 Preparación para la construcción, pruebas y despliegue
- ST 4.4.5.3 Construcción y pruebas
- ST 4.4.5.4 Pruebas y pilotos del servicio
- ST 4.4.5.5 Planificar y preparar el despliegue

Las buenas prácticas sugieren:

COBIT 4.1: Sugiere tener un plan de implantación y respaldo y vuelta atrás.

ITIL V3: Sugiere recopilar todos los componentes de la versión y de poner a punto el entorno de pruebas en las condiciones necesarias para su correcto desarrollo.

AI7.4 AMBIENTE DE PRUEBA

Relación con otros estándares:

ITIL V3:

- ST 3.2.14 Mejora proactiva de la calidad durante la transición del servicio
- ST 4.4.5.2 Preparación para la construcción, pruebas y despliegue
- ST 4.4.5.3 Construcción y pruebas
- ST 4.4.5.4 Pruebas y pilotos del servicio

ISO 27002:

- 10.1.4 Separación de los entornos de desarrollo, pruebas y producción
- 12.4.3 Control de acceso al código fuente de los programas
- 12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo

Las buenas prácticas sugieren:

COBIT 4.1: Sugiere definir y establecer un entorno seguro relativos a controles internos

ITIL V3: La fiabilidad de las pruebas está condicionada al entorno en el que éstas tienen lugar. Si no es idéntico al escenario real en que se desplegará el servicio nuevo o modificado, los resultados de las pruebas se verán distorsionados y por tanto no servirán.

ISO 27002: Sugiere identificar e implementar controles adecuados para el nivel de separación entre los entornos de desarrollo, prueba y producción que es necesario para

evitar problemas operacionales. Las actividades de desarrollo y prueba pueden causar serios problemas, por ejemplo, cambios no deseados en los archivos o en el entorno del sistema o fallos del sistema. En este caso es necesario mantener un entorno conocido y estable para poder realizar las pruebas significativas y evitar el acceso inapropiado del personal de desarrollo. Si el personal de desarrollo y el de prueba tuvieran acceso al sistema de producción y a su información, podrían introducir un código no autorizado o no probado o alterar los datos operacionales.

AI7.6 PRUEBAS DE CAMBIOS

Relación con otros estándares:

ITIL V3:

- ST 3.2.14 Mejora proactiva de la calidad durante la transición del servicio
- ST 4.4.5.4 Pruebas y pilotos del servicio
- ST 4.5.5.5 Ejecutar pruebas
- ST 4.5.5.6 Evaluar criterios de fin de pruebas y reportar

ISO 27002:

- 6.1.4 Proceso de autorización para las instalaciones de procesamiento de información
- 12.4.3 Control de acceso al código fuente de los programas
- 12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo

Las buenas prácticas sugieren:

COBIT 4.1: Sugiere que independientemente a los planes de pruebas definir antes de la migración el entorno de operaciones y asegurarse que el plan considera la seguridad y el desempeño

ITIL V3: En esta etapa del proceso se llevan a cabo las pruebas propiamente dichas: todos los componentes, herramientas y mecanismos que participan en el despliegue, la migración, son examinados uno por uno. El desarrollo de las pruebas puede ser automático o manual

ISO 27002: Sugiere revisar y probar las aplicaciones críticas de negocio cuando se realicen cambios en el sistema, con objeto de garantizar que no existen impactos adversos para las actividades o seguridad de la Organización

AI7.7 PRUEBA DE ACEPTACIÓN FINAL

Relación con otros estándares:

ITIL V3:

- ST 4.4.5.4 Pruebas y pilotos del servicio
- ST 4.5.5.5 Ejecutar pruebas
- ST 4.5.5.6 Evaluar criterios de salida y reportar

ISO 27002:

- 10.3.2 Aceptación del sistema

- 12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo
- 12.5.4 Fuga de información

Las buenas prácticas sugieren:

COBIT 4.1: Sugiere que el dueño de proceso de negocio y los interesados de TI evalúen los resultados de los procesos de prueba y redimir los errores significativos identificados en el proceso de prueba.

ITIL V3: Sugiere en comparar los datos reales obtenidos en las pruebas con los criterios de aceptación de servicio, si la versión no cumple los requisitos mínimos preestablecidos, es devuelta como “no aceptada” a la Gestión de Cambios para su reevaluación. En cambio, si el análisis es favorable y existen garantías de que la versión cumple las condiciones necesarias para obtener el consentimiento del cliente, se procede a la elaboración de un informe completo de resultados de las pruebas.

ISO 27002: Sugiere establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y versiones nuevas, como también desarrollar las pruebas adecuadas del sistema durante el desarrollo y antes de su aceptación

AI7.9 REVISIÓN POSTERIOR A LA IMPLANTACIÓN

Relación con otros estándares:

ITIL V3:

- ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado
- ST 4.1.5.3 Planear y coordinar la transición del servicio
- ST 4.4.5.10 Revisar y cerrar la transición del servicio
- ST 4.4.5.7 Verificar despliegue
- ST 4.4.5.9 Revisar y cerrar un despliegue
- ST 4.6 Evaluación
- SO 4.3.5.5 Cierre

Las buenas prácticas sugieren:

COBIT 4.1: Sugiere establecer procedimientos en línea con los estándares correctos de gestión de cambios organizacionales

ITIL V3: Sugiere proceder a la limpieza del entorno de pruebas, revirtiendo los cambios incorporados durante los test (instalación de aplicaciones, importación de datos, etc.) hasta la situación inicial. En esta última etapa, el equipo encargado de las pruebas revisa el planteamiento de las mismas y verifica si la planificación se cumplió conforme a los recursos, criterios de aceptación de servicio y plazos acordados. Así, se detectan aspectos mejorables para perfeccionar el proceso.

DS5 – GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS

DS5.3 ADMINISTRACIÓN DE IDENTIDAD

Relación con otros estándares:

ITIL V3:

- 4.5.5.4 Supervisión del régimen de la identidad

ISO 27002:

- 11.2.3 Gestión de contraseña de usuarios
- 11.3.1 Uso de contraseñas
- 11.5.2 Identificación y autenticación de usuario
- 12.3.2 Gestión de claves

Las buenas prácticas sugieren:

COBIT 4.1. Sugiere asegurar que todos los usuarios y su actividad en sistemas de TI, deben ser identificables de manera única. Además permitir que todos los usuarios se identifiquen a través de mecanismos de autenticación. Junto a estos, se sugiere confirmar que los permisos de acceso del usuario al sistema y los datos, estén alineados con las necesidades del negocio.

ITIL V3. Sugiere gestionar los accesos, que debe comprender y documentar el ciclo de vida típico de usuario, para cada tipo de usuario y utilizarlo para automatizar el proceso. Las gestiones de acceso son las herramientas que proporcionan funciones que permiten a un

usuario se mueve de un estado a otro, o de un grupo a otro, fácilmente y con una pista de auditoría.

ISO 27002. Sugiere establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información. Además los usuarios deberían ser conscientes de sus responsabilidades en el mantenimiento de controles de acceso eficaces. En particular, respecto al uso de contraseñas y seguridad en los equipos puestos a su disposición, teniendo en cuenta las prestaciones de seguridad del sistema, que deberían ser capaces de la autenticación de los usuarios autorizados, de acuerdo a la política de control de acceso definida.

DS5.4 ADMINISTRACIÓN DE CUENTAS DE USUARIO

Relación con otros estándares:

ITIL V3:

- 4.5.5.1 Solicitud de acceso
- 4.5.5.3 Proporcionar los derechos
- 4.5.5.5 Registro y seguimiento del acceso
- 4.5.5.6 Eliminación o restricción de los derechos

ISO 27002:

- 11.1.1 Políticas de control de acceso
- 11.2.1 Registro de usuario
- 11.2.2 Gestión de privilegios

- 11.5.1 Procedimientos seguros de inicio de sesión

Las buenas prácticas sugieren:

COBIT 4.1: Sugiere garantizar que la solicitud, establecimiento, emisión, modificación y cierre de cuentas y de los privilegios relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuario, además de incluir procedimientos de aprobación que describa el responsable de los datos o del sistema otorgando los privilegios de acceso, y dichos procedimientos deben aplicarse a todos los usuarios.

ITIL V3. Sugiere gestionar los accesos, que debe comprender y documentar el ciclo de vida típico de usuario, para cada tipo de usuario y utilizarlo para automatizar el proceso. Las gestiones de acceso son las herramientas que proporcionan funciones que permiten a un usuario se mueve de un estado a otro, o de un grupo a otro, fácilmente y con una pista de auditoría.

ISO 27002: Sugiere establecer un procedimiento formal de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información. Además sugiere restringir y controlar la asignación y uso de los privilegios y controlar el acceso al sistema operativo mediante procedimientos seguros de conexión.

11.7 NIVEL DE MADUREZ PARA CADA PROCESO COBIT 4.1

UNIVERSIDAD DE LA COSTA

NIVEL DE MADUREZ DE LOS PROCESO COBIT 4.1 SELECCIONADOS

AUDITORIA AL MODULO DE CONSULTA EXTERNA DEL SISTEMA DE INFORMACIÓN MEDULA DE LA EMPRESA COMPGENIOSS LTDA.

Ingeniero: Bladimir Cahuana

Julio de 2012

NIVEL DE MADUREZ

ESQUEMA DEFINIDO POR EL MARCO DE REFERENCIA COBIT 4.1

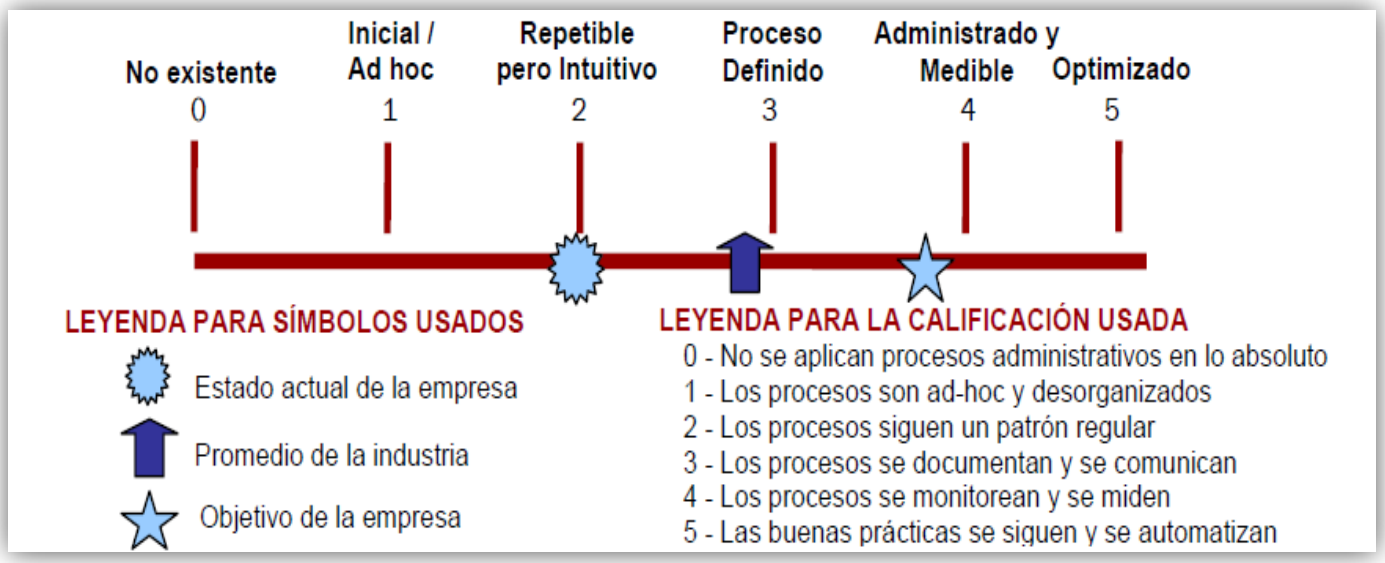


Figura 9. Representación grafica de los modelos de madurez COBIT 4.1

0 No Existente- Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

1 Inicial- Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

2 Repetible- Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

3 Definido- Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

4 Administrado- Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

5 Optimizado- Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Figura 10. Modelo genérico de madurez COBIT 4.1

NIVEL DE MADUREZ DE LOS PROCESOS SELECCIONADOS

OBJETIVO DE CONTROL: PO3 Determinar la Dirección Tecnológica

CRITERIOS DE INFORMACIÓN

PRIMARIOS: Efectividad, Eficiencia

ÁREAS DE ENFOQUE DEL GOBIERNO DE TI

PRIMARIOS: Administración de Recursos

SECUNDARIOS: Alineación Estratégica, Entrega de Valor, Administración de Riesgos

RECURSOS DE TI

Enfocado a las aplicaciones e Infraestructura

NIVEL DE MADUREZ

No existente

No se encuentran establecidas las normas y políticas de seguridad del aplicativo, establecidas por la ley, además de la documentación necesaria, para la legalización de los derechos de autor del aplicativo MEDULA, pero las directivas ya identificaron esta falencia en sus procesos y ya empezaron a tomar los correctivos necesarios para cumplir con todas las normas y solicitudes que el estado pide al momento de desarrollar y comercializar este tipo de productos.

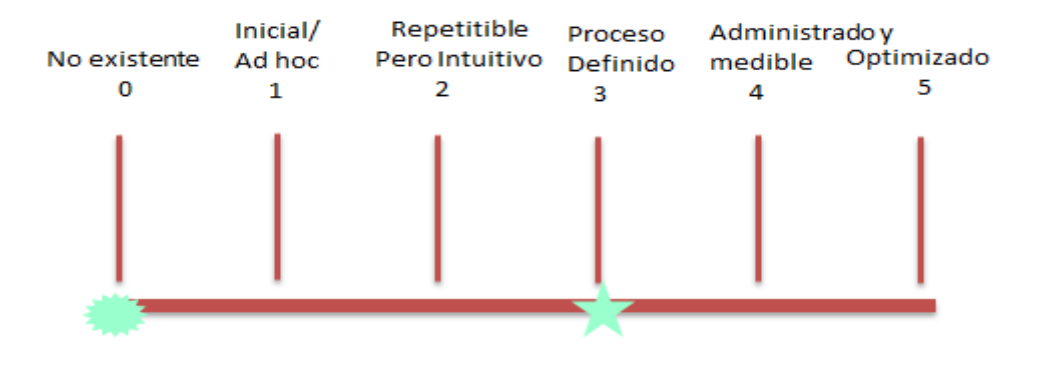


Figura 11. Representación gráfica del nivel de madurez del Proceso PO3

OBJETIVO DE CONTROL: PO9 Evaluar y administrar los riesgos de TI

CRITERIOS DE INFORMACIÓN

PRIMARIOS: Confidencialidad, Integridad, Disponibilidad

SECUNDARIOS: Efectividad, Eficiencia, Cumplimiento, Confiabilidad

ÁREAS DE ENFOQUE DEL GOBIERNO DE TI

PRIMARIOS: Administración de Riesgos, Alineación estratégica,

RECURSOS DE TI

Enfocado a las aplicaciones, Información, Infraestructura y personas

NIVEL DE MADUREZ

No existente

No se cuenta con un plan de acción de riesgos debidamente elaborado para el aplicativo MEDULA lo cual es sumamente grave así como también lo es el hecho de que nunca se evaluó la probabilidad de ocurrencia e impacto de los riesgos que se podrían presentar aunque se tenían conciencia y una leve idea de los eventos no deseados que podrían ocurrir.

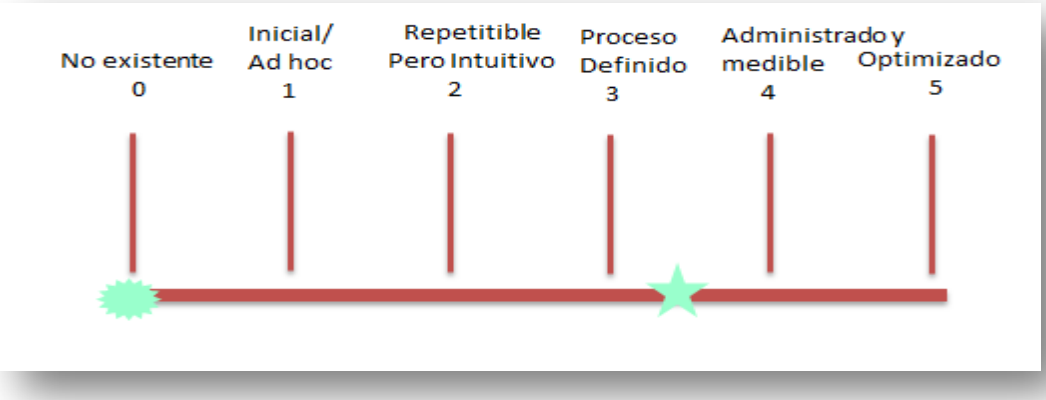


Figura 12. Representación gráfica del nivel de madurez del Proceso PO9

OBJETIVO DE CONTROL: PO10 Administrar proyectos

CRITERIOS DE INFORMACIÓN

PRIMARIOS: Efectividad, Eficiencia

ÁREAS DE ENFOQUE DEL GOBIERNO DE TI

PRIMARIOS: Alineación estratégica,

SECUNDARIOS: Entrega de valor, Administración de Riesgos, Administración de recursos, Medición del desempeño

RECURSOS DE TI

Enfocado a las aplicaciones, Infraestructura y personas

NIVEL DE MADUREZ

No existente

No existe una política formal y claramente definida para el desarrollo de nuevos proyectos, la decisión de emprender el proyecto del sistema de información MEDULA fue tomada única y exclusivamente por el Gerente General, sin contar con una metodología a seguir por lo tanto no se tuvo control sobre el presupuesto, el cronograma y los entregables.

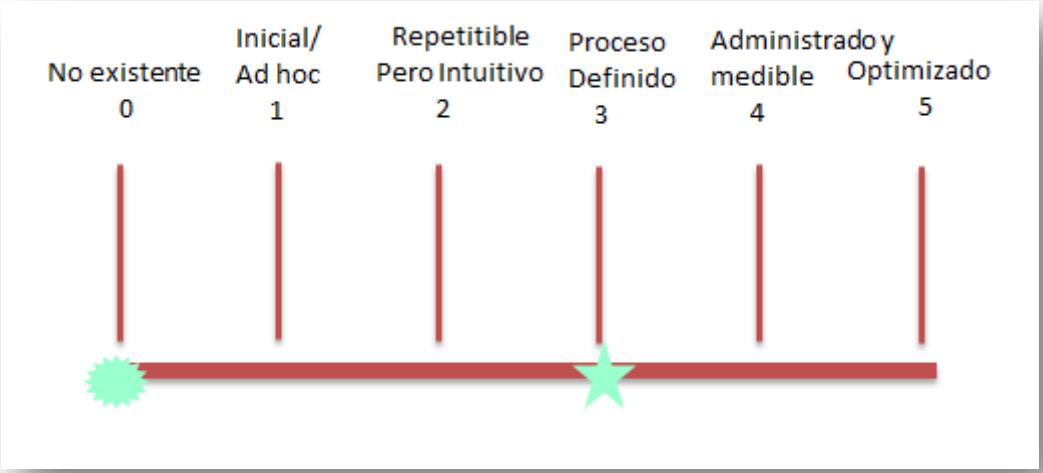


Figura 13.Representación gráfica del nivel de madurez del Proceso PO10

OBJETIVO DE CONTROL: AI2 Adquirir y mantener software aplicativo

CRITERIOS DE INFORMACIÓN

PRIMARIOS: Efectividad, Eficiencia

SECUNDARIOS: Integridad, Confiabilidad

ÁREAS DE ENFOQUE DEL GOBIERNO DE TI

PRIMARIOS: Entrega de valor, Alineación estratégica

SECUNDARIOS: Administración de Riesgos

RECURSOS DE TI

Enfocado a las aplicaciones

NIVEL DE MADUREZ

Inicial/Ad Hoc

Existe conciencia mínima sobre las reglamentaciones y metodologías que se deben tener presente cuando se adquiere o implementan recursos de TI en CompGenioss, se realiza un análisis de las necesidades del negocio para ver que producto se debe adquirir y se realizan mantenimientos periódicos pero no controlados de los recursos.

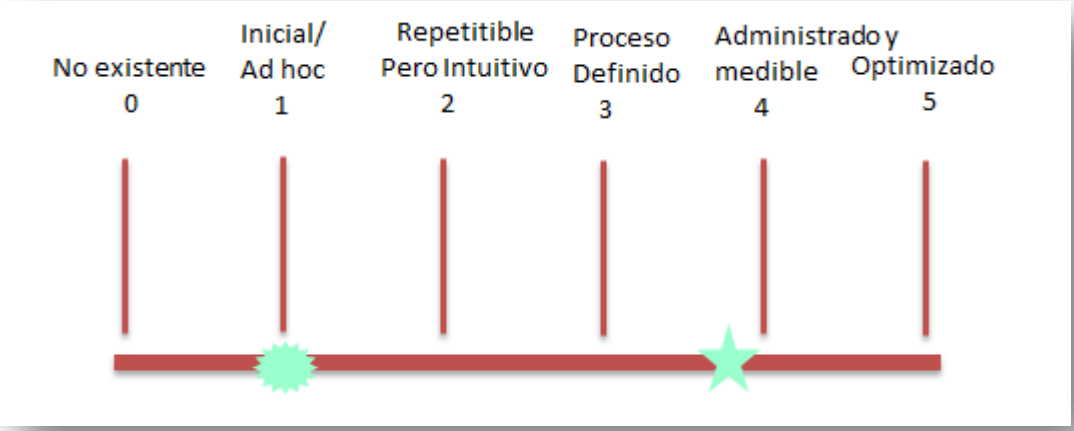


Figura 14. Representación gráfica del nivel de madurez del Proceso AI2

OBJETIVO DE CONTROL: AI4 Facilitar la Operación y el Uso

CRITERIOS DE INFORMACIÓN

PRIMARIOS: Efectividad y Eficiencia

SECUNDARIOS: Integridad, Disponibilidad, Cumplimiento y Confiabilidad

ÁREAS DE ENFOQUE DEL GOBIERNO DE TI

PRIMARIOS: Entrega de Valor

SECUNDARIOS: Alineación Estratégica, Administración de Riesgos, Administración de Recursos

RECURSOS DE TI

Enfocado a las aplicaciones, Infraestructura y personas

NIVEL DE MADUREZ

Inicial/ Ad Hoc

No se cuenta con documentación sobre el aplicativo MEDULA, así como tampoco se tienen los manuales de usuario y manuales de operación y soporte, solo se tienen diapositivas, que contienen un breve resumen del funcionamiento general del aplicativo. Los nuevos usuarios que ingresan, no tienen un debido entrenamiento, solo son informados de forma verbal, de algunos temas relacionados al manejo del aplicativo. Aunque ya la gerencia, se encuentra al tanto de estas fallas, y se encuentran trabajando en las respectivas mejoras, con respecto a este tema.

Figura 15. Representación gráfica del nivel de madurez del Proceso AI4

OBJETIVO DE CONTROL: AI5 Adquirir Recursos de TI

CRITERIOS DE INFORMACIÓN

PRIMARIOS: Eficiencia

SECUNDARIOS: Efectividad, Cumplimiento

ÁREAS DE ENFOQUE DEL GOBIERNO DE TI

PRIMARIOS: Administración de Recursos

SECUNDARIOS: Entrega de valor

RECURSOS DE TI

Enfocado a las aplicaciones, Información, Infraestructura y personas

NIVEL DE MADUREZ

Repetible pero intuitivo

Para la adquisición de recursos de TI no existen procesos o metodologías definidas, pero se realizan investigación sobre los productos que ofrece el mercado se hace una relación costo/beneficio el problema está en que el factor más determinante para la adquisición es el reconocimiento de la marca, sin embargo se requiere autorización previa del gerente General al momento de adquirir nuevos recursos para el desarrollo de las actividades de la empresa.

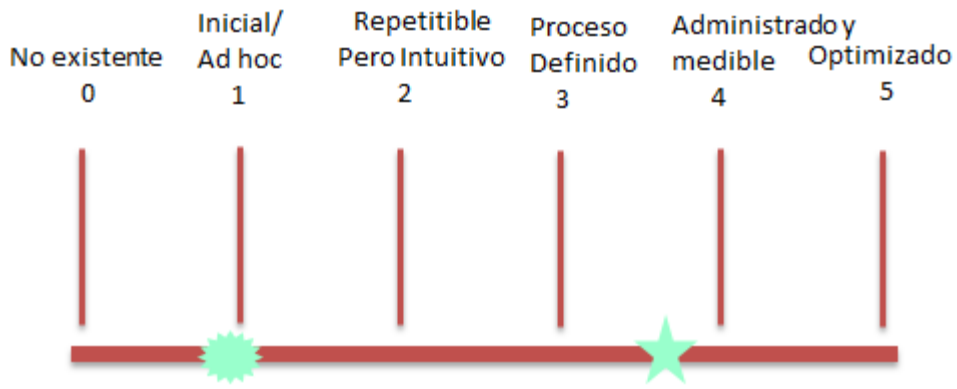


Figura 16. Representación gráfica del nivel de madurez del Proceso AI5

OBJETIVO DE CONTROL: AI6 Administrar Cambios

CRITERIOS DE INFORMACIÓN

PRIMARIOS: Efectividad, Eficiencia, Integridad

ÁREAS DE ENFOQUE DEL GOBIERNO DE TI

PRIMARIOS: Medición del desempeño

SECUNDARIOS: Entrega de valor

RECURSOS DE TI

Enfocado a las aplicaciones, Información y personas

NIVEL DE MADUREZ

Inicial/ Ad Hoc

No existe un proceso de administración de cambio formal en la organización, por lo tanto se efectuan cambios en el aplicativo sin la autorizacion previa del gerente de operación tecnologica, solo se realizan las pruebas y se hacen los respectivos cambios pero no existe documentación del mismo.

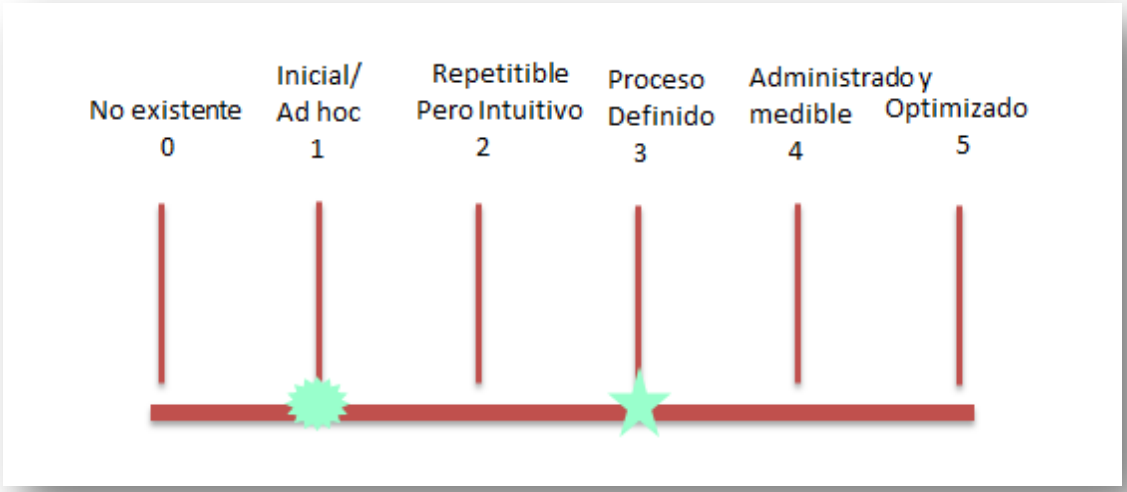


Figura 17. Representación gráfica del nivel de madurez del Proceso AI6

OBJETIVO DE CONTROL: AI7 Instalar Y Acreditar Soluciones Y Cambios

CRITERIOS DE INFORMACIÓN

PRIMARIOS: Efectividad, Eficiencia, Integridad

SECUNDARIOS: Disponibilidad, Confiabilidad

ÁREAS DE ENFOQUE DEL GOBIERNO DE TI

PRIMARIOS: Medición del desempeño, Entrega de valor

SECUNDARIOS: Alineación estratégica, Administración de Riesgos, Administración de recursos

RECURSOS DE TI

Enfocado a las aplicaciones, Infraestructura, Información y personas

NIVEL DE MADUREZ

No existente

No existe un proceso formal para la instalación y acreditación de soluciones y cambios en la organización, por lo cual los desarrolladores son los que efectuan las pruebas en base a su experiencia y deciden en que momento realizarlas. En ocaciones se evalúan y se aprueban los resultados de las pruebas por parte de la gerencia de la compañía.

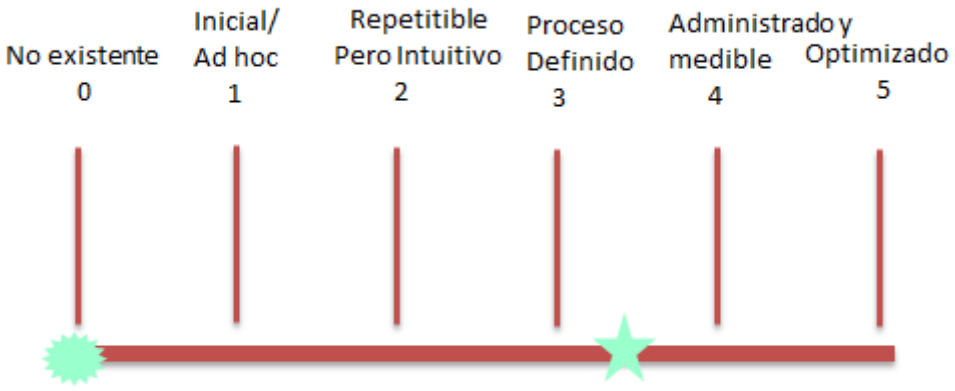


Figura 18. Representación gráfica del nivel de madurez del Proceso AI7

OBJETIVO DE CONTROL: DS5 Garantizar la Seguridad de los Sistemas

CRITERIOS DE INFORMACIÓN

PRIMARIOS: Confidencialidad e Integridad

SECUNDARIOS: Disponibilidad, Cumplimiento y Confiabilidad

ÁREAS DE ENFOQUE DEL GOBIERNO DE TI

PRIMARIOS: Administración de Riesgos

RECURSOS DE TI

Enfocado a las aplicaciones, Infraestructura y personas

NIVEL DE MADUREZ

Inicial/ Ad Hoc

No se cuenta con una matriz definida de roles y perfiles de usuarios, ya que en el aplicativo MEDULA, no se encuentran bien definidos los permisos y accesos de los diferentes usuarios que existen en el sistema. El aplicativo cuenta con un rol administrador, con todos los privilegios, pero los demás usuarios (Usuarios Normales), tienen en su gran mayoría los mismos privilegios. Además el aplicativo cuenta con un sistema de autenticación de usuarios, que permite controlar el acceso al sistema. La gerencia de operaciones se encuentra realizando pruebas y acciones correctivas, que permitan mejorar la seguridad del aplicativo.

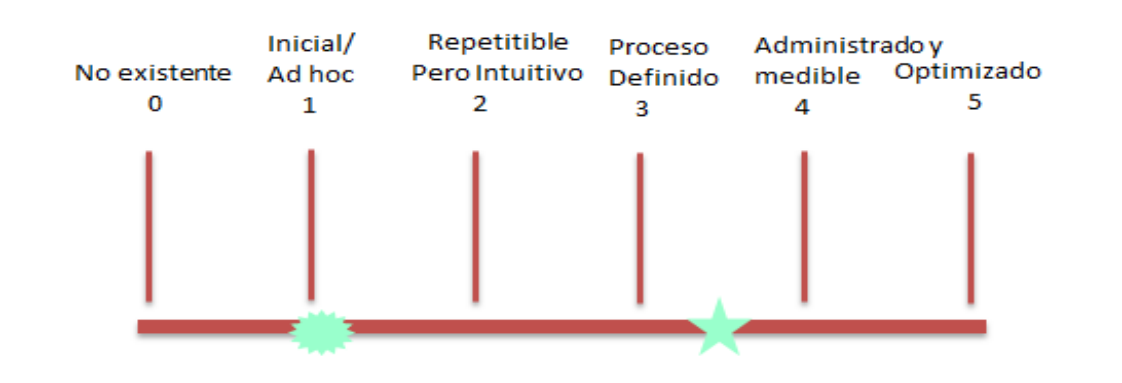


Figura 19. Representación gráfica del nivel de madurez del Proceso DS5

12. CONCLUSIÓN

Hoy, como cada organización trata de entregar valor a través de TI, a la vez que gestiona un complejo rango de riesgos relacionados a TI, el uso efectivo de las mejores prácticas puede ayudar a evitar la reinvención de sus propias políticas y procedimientos, optimizando el uso de escasos recursos de TI y reduciendo la incidencia de los mayores riesgos de TI, tales como: Proyectos fallidos, Inversiones perdidas, Brechas de seguridad, Fallas de los sistemas, Fallas de proveedores para entender y satisfacer los requerimientos de los clientes.

Brindar a sus actuales y futuros clientes un software de calidad motivó a COMPGENIOSS LTDA. a la realización de una auditoria al sistema de información MEDULA, específicamente al módulo de consulta externa, la cual consistió en la evaluación y verificación de los controles, la integridad y confidencialidad de los datos, accesos y perfiles al sistema, interfaces y posibles errores o fallas del aplicativo.

Se utilizaron los marcos de referencias COBIT 4.1, ISO 27002, ITIL V3, e ISO 3100, obteniendo de ellos varios controles, procesos y métodos de estos estándares. La ventaja de utilizar e implementar estos estándares es que se puede percibir de una forma sencilla que tan lejos o cerca está la compañía de una buena práctica, las cuales son un punto de partida importante a la hora de crear y proteger la información.

Identificar posibles riesgos y proponer alternativas de solución a la empresa fue uno de los objetivos de la auditoria que con el apoyo de estándares que soportados en buenas prácticas y utilizando conocimientos teóricos, enfocado específicamente del marco de

referencia COBIT 4.1 permitió la administración del riesgo y el nivel de madurez del aplicativo.

Este proyecto buscó en COMPGENIOSS LTDA. Un lineamiento que le permita conocer los beneficios que tiene la adopción eficaz de las mejores prácticas, lo cual redundará en obtener valor de las inversiones y los servicios de TI permitiendo así a la organización: Mejorar la calidad, la respuesta y la fiabilidad de las soluciones y los servicios de TI, Mejorar la viabilidad, previsibilidad y repetitividad de resultados de negocio exitosos, Reducir riesgos, incidentes y fallas en los proyectos.

13. BIBLIOGRAFÍA

- Mejores prácticas de la auditoría en informática, Capítulo 3. Legislación informática, mejores prácticas y técnicas de auditoría informática
- Comité Directivo de COBIT y la Information Systems Audit and Control Foundation. COBIT Directrices De Auditoria. 2da Edición. 1998.
- IT Governance Institute. COBIT 4.1. 2007
- IT Governance Institute. Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa.2008
- ISO/FDIS 3100: 2009 (E). La gestión de riesgos-principios y directrices.
- Norma Técnica Colombiana NTC-ISO/IEC 2700. Tecnología de la información, Técnicas de seguridad, Gestión del riesgo en la seguridad de la información. 2009-08-19
- http://www.veeduriadistrital.gov.co/es/grupo/g285/web/Archivo2AS.pdf
- http://www.gerencie.com/auditoria-de-sistemas-de-informacion.html
- http://www.formaselect.com/curso/experto-en-sql-server-2000/Introduccion-a-SQL-Server%202000.pdf
- http://www.intercambiosvirtuales.org/software/microsoft-sql-server-2008-r2-enterprise-edition-dvd-espanol
- http://www.soyentrepreneur.com/cobit-41-reduce-riesgos-y-mejora-desempeno-de-las-ti.html

- http://www.tgti.es/?q=node/151
- http://www.slideshare.net/RMVTITO/cobit-41-3875960Ç
- http://www.docstoc.com/docs/47377807/Benefits-of-Data-Analysis-Techniques

ANEXO 1
CARTA DE ENTREGA Y AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO DE TESIS Y TRABAJOS DE GRADO

Barranquilla, 12 de Octubre de 2012

Marque con una X
Tesis ■ **Trabajo de Grado** □

Yo IRLETH KARINE FONSECA ZAMBRANO, identificado con C.C. No. 1043001010, actuando en nombre propio y como autor de la tesis y/o trabajo de grado titulado AUDITORIA AL MODULO DE CONSULTA EXTERNA DEL SISTEMA DE INFORMACION MEDULA DE LA EMPRESA COMPGENIOSS LTDA presentado y aprobado en el año 2012 como requisito para optar al título de Especialista en Auditoria de Sistemas de Información;
hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (DVD) y autorizo a la UNIVERSIDAD DE LA COSTA, CUC, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

Y autorizo a la Unidad de información, para que con fines académicos, muestre al mundo la producción intelectual de la Universidad de la Costa, CUC, a través de la visibilidad de su contenido de la siguiente manera:

Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Unidad de información, en el repositorio institucional y en las redes de información del país y del exterior, con las cuales tenga convenio la institución y Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato DVD o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTES, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los 12 días del mes de OCTUBRE de Dos Mil DOCE 2012

EL AUTOR - ESTUDIANTE. IRLETH FONSECA ZAMBRANO
FIRMA

ANEXO 1
CARTA DE ENTREGA Y AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO DE TESIS Y TRABAJOS DE GRADO

Barranquilla, 12 de Octubre de 2012

Marque con una X
Tesis ■ **Trabajo de Grado** □

Yo ALCIDES DE JESUS GIOVANNETTI CAHUANA, identificado con C.C. No. 1042349216, actuando en nombre propio y como autor de la tesis y/o trabajo de grado titulado AUDITORIA AL MODULO DE CONSULTA EXTERNA DEL SISTEMA DE INFORMACION MEDULA DE LA EMPRESA COMPGENIOSS LTDA presentado y aprobado en el año 2012 como requisito para optar al título de Especialista en Auditoria de Sistemas de Información;
hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (DVD) y autorizo a la UNIVERSIDAD DE LA COSTA, CUC, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

Y autorizo a la Unidad de información, para que con fines académicos, muestre al mundo la producción intelectual de la Universidad de la Costa, CUC, a través de la visibilidad de su contenido de la siguiente manera:

Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Unidad de información, en el repositorio institucional y en las redes de información del país y del exterior, con las cuales tenga convenio la institución y Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato DVD o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTES, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los 12 días del mes de OCTUBRE de Dos Mil DOCE 2012

EL AUTOR - ESTUDIANTE. ALCIDES GIOVANNETTI CAHUANA
FIRMA

ANEXO 1
CARTA DE ENTREGA Y AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO DE TESIS Y TRABAJOS DE GRADO

Barranquilla, 12 de Octubre de 2012

Marque con una X
Tesis ■ **Trabajo de Grado** □

Yo JOSE LUIS REDONDO AGUILAR, identificado con C.C. No. 1129513615, actuando en nombre propio y como autor de la tesis y/o trabajo de grado titulado AUDITORIA AL MODULO DE CONSULTA EXTERNA DEL SISTEMA DE INFORMACION MEDULA DE LA EMPRESA COMPGENIOSS LTDA presentado y aprobado en el año 2012 como requisito para optar al título de Especialista en Auditoria de Sistemas de Información;
hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (DVD) y autorizo a la UNIVERSIDAD DE LA COSTA, CUC, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

Y autorizo a la Unidad de información, para que con fines académicos, muestre al mundo la producción intelectual de la Universidad de la Costa, CUC, a través de la visibilidad de su contenido de la siguiente manera:

Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Unidad de información, en el repositorio institucional y en las redes de información del país y del exterior, con las cuales tenga convenio la institución y Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato DVD o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTES, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los 12 días del mes de OCTUBRE de Dos Mil DOCE 2012

EL AUTOR - ESTUDIANTE. JOSE REDONDO AGUILAR
FIRMA

-

ANEXO 2
FORMULARIO DE LA DESCRIPCIÓN DE LA TESIS O DEL TRABAJO DE GRADO

TÍTULO COMPLETO DE LA TESIS O TRABAJO DE GRADO:

AUDITORIA AL MODULO DE CONSULTA EXTERNA DEL SISTEMA DE INFORMACION MEDULA DE LA EMPRESA COMPGENIOSS LTDA

SUBTÍTULO, SI LO TIENE:

AUTOR AUTORES

Apellidos Completos	Nombres Completos
Fonseca Zambrano Giovannetti Cahuana Redondo Aguilar	Irleth Karine Alcides de Jesus Jose Luis

DIRECTOR (ES)

Apellidos Completos	Nombres Completos
Montaño Ardila	Victor Manuel

JURADO (S)

Apellidos Completos	Nombres Completos
MARTINEZ OROZCO	UBALDO MARIO

ASESOR (ES) O CODIRECTOR

Apellidos Completos	Nombres Completos
Barraza Olaya	Telma

TRABAJO PARA OPTAR AL TÍTULO DE: Especialista en Auditoria de Sistemas de Información

FACULTAD: Ciencias Económicas

PROGRAMA: Pregrado ____ Especialización X

NOMBRE DEL PROGRAMA Especialización en Auditoria de Sistemas de Información

CIUDAD: Barranquilla **AÑO DE PRESENTACIÓN DEL TRABAJO DE GRADO:** 2012

NÚMERO DE PÁGINAS 219

TIPO DE ILUSTRACIONES:

- ☐ Ilustraciones
- ☐ Láminas
- ☐ Retratos
- ☒ Tablas, gráficos y diagramas
- ☐ Planos
- ☐ Mapas
- ☐ Fotografías

MATERIAL ANEXO (Vídeo, audio, multimedia o producción electrónica):
Duración del audiovisual: _____ minutos.

Número de casetes de vídeo: _____ Formato: VHS ___ Beta Max ___ ¾ ___ Beta Cam ____

Mini DV ____ DV Cam ____ DVC Pro ____ Vídeo 8 ____ Hi 8 ____

Otro. Cuál? _____

Sistema: Americano NTSC _____ Europeo PAL _____ SECAM _____

Número de casetes de audio: _____

Número de archivos dentro del DVD (En caso de incluirse un DVD diferente al trabajo de grado):

_____

PREMIO O DISTINCIÓN *(En caso de ser LAUREADAS o tener una mención especial)*:

_____

DESCRIPTORES O PALABRAS CLAVES EN ESPAÑOL E INGLÉS: Son los términos que definen los temas que identifican el contenido. (*En caso de duda para designar estos descriptores, se recomienda consultar con la Unidad de Procesos Técnicos de la Unidad de información en el correo biblioteca@cuc.edu.co, donde se les orientará).*

ESPAÑOL	**INGLÉS**
Riesgo, Auditoria, Sistema, Informacion	Risk, Audit, System, Informacion, Security
Seguridad, Cobit, Itil, Iso,Nivel de madurez	Cobit, Itil, Iso, Maturity level, Processes
Procesos, Organizacion	Organization

RESUMEN DEL CONTENIDO EN ESPAÑOL E INGLÉS:(Máximo 250 palabras-1530 caracteres):

Esta auditoría consistió en realizar la evaluación y verificación de los controles, la integridad y confidencialidad de los datos, accesos y perfiles al sistema, interfaces y posibles errores o fallas del aplicativo, utilizando como Marco de Referencia COBIT 4.1 el cual se complementó con ISO 27002, ITIL V3, ISO 3100.

This audit was to conduct the evaluation and testing of controls, integrity and confidentiality of data, and access to the system profiles, interfaces and possible errors or failures of the application, using COBIT 4.1 framework which complement with ISO 27002, ITIL V3, ISO3100.