Trabajo Final de Graduación

APLICACIÓN DE NORMAS ISO 17799 Y COBIT DE LA SEGURIDAD LÓGICA EN LA EMPRESA AGUA DE LOS ANDES S.A.

CARACINO JOSÉ LUIS

LICENCIATURA EN INFORMÁTICA

UNIVERSIDAD EMPRESARIAL SIGLO 21

2012

Resumen

El presente Trabajo Final de Graduación tiene por objeto exponer a las autoridades de la Empresa Agua de los Andes S.A. la importancia de la Seguridad Informática con el fin de movilizarlos a realizar mejoras, controles y rendimientos de los sistemas informáticos para minimizar los posibles daños a la organización y prevenir riesgos que puedan impedir el normal funcionamiento.

Para ello en primera instancia se realizo un relevamiento en cuanto a riesgos informáticos en el departamento de Informática aplicando Normas ISO 17799.

Luego se analizaron los riesgos lógicos existentes integrando los objetivos de control de COBIT y la norma ISO/IECE 17799-2005 mapeando estos con las cláusulas de control de seguridad de la norma ISO, procediendo a la elaboración de modelos de madurez indicando con ello el grado de madurez y objetivos no cumplidos en cada uno de los procesos que establece COBIT.

Finalmente se identificaron los factores de riesgo y se plantearon recomendaciones que si bien no ofrecen la solución, contribuyeron a la identificación de las debilidades encontradas.

Palabras Clave: Seguridad Informática, Relevamiento, Objetivos de Control, Modelos de Madurez, Factores de Riesgo, Recomendaciones.

Abstract

This Final Graduation Work aims to expose to the authorities of Agua de los Andes S. A. the importance of informatics security in order to mobilize them to make improvements, controls and performance of computer systems to minimize potential damage to the organization and prevent risks that may impede the normal operation.

This was done in the first instance as a study regarding the informatics threats in its department applying the rules ISO 17799.

Then the logic existing risks were analyzed by integrating the COBIT control objectives and the ISO / IECE 17799-2005 rule and mapping these to the security control clauses of the ISO rule. Later it was preceded with the development of maturity models thus indicating the degree of maturity and unfulfilled targets in each of the processes established by COBIT.

Finally, risk factors were identified and recommendations were drawn while not offering a solution, contributed to the identification of the weaknesses founded.

Keywords: Computer Security, Survey, Control Objectives, Maturity Models, Risk Factors, Recommendations.

INDICE

1.- Introducción del Trabajo Final de Graduación

Aplicación de normas ISO 17799 y COBIT para el diagnóstico de la Seguridad Lógica Informática en la Empresa Agua de los Andes S.A.

Este Trabajo Final de Graduación (T.F.G.) se realizó luego de conocer la importancia que tiene el manejo de la información en la vida empresarial, esta información es fundamental tanto en organizaciones grandes como pequeñas ya que es considerada como un activo más; conociendo este aspecto se realizó este trabajo, el cual trata el estudio de la seguridad lógica de dicho departamento.

1.1. Formulación del problema

La información es un activo esencial para el negocio de la organización y en consecuencia necesita ser protegido adecuadamente. Como resultado de la creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades

La seguridad de la información depende de la protección de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo y maximizar el retorno de las inversiones.

Esto se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y un apropiado software. Se necesitan establecer, implementar, monitorear, revisar y

mejorar estos controles para asegurar que se cumplan objetivos específicos de seguridad

Los requerimientos se identifican mediante una evaluación metódica de los riesgos. El gasto en controles debe ser equilibrado con el daño probable resultante de fallas en la seguridad.

Los resultados de la evaluación del riesgo ayudarán a guiar y determinar la acción de gestión apropiada y las prioridades para manejarlos, e implementar controles para protegerse de los mismos

Esta operatoria se debe repetir periódicamente para tratar cualquier cambio que puede influir en los resultados de la evaluación del riesgo.

1.2. Alcance del T.F.G.

1.2.1. Limite y Alcance

En el presente T.F.G. se aplicaron Normas ISO 17799 y COBIT como metodología para el análisis de la situación actual del Departamento de Informática de la organización Agua de los Andes S.A., explicando si se respetan procedimientos conforme a las normas, e indicando factores de riego y recomendaciones que si bien no ofrecen la solución, contribuirán a la identificación de las debilidades en la Seguridad Lógica de la Empresa.

1.2.2. Justificación

En la actualidad las empresas privadas han experimentado transformaciones en algunos aspectos de seguridad; la situación actual nos da a conocer que los sistemas informáticos son el activo más valioso y al mismo tiempo el más vulnerable.

La seguridad informática ha adquirido gran auge, dada las cambiantes condiciones y nuevas plataformas de computación disponibles, situación que converge en la aparición de nuevas amenazas en los sistemas informáticos.

Dada la problemática planteada, se realizó un control interno de seguridad lógica aplicando COBIT y Normas ISO 17799 con el objeto de hacer notar a las autoridades de la empresa lo importante que es la aplicación de la seguridad informática y la poca importancia que se le da, también con el fin de movilizar a los involucrados a realizar mejoras, control y rendimiento de los sistemas informáticos, para minimizar los posibles daños a la organización y prevenir riesgos que puedan impedir el normal funcionamiento de la Empresa.

1.2.3. Objetivo General

El presente T.F.G. se tomaron en cuenta Normas ISO 17799 y COBIT como parámetro de análisis de la situación en que se encuentra el Departamento Informática de la Empresa Agua de los Andes S.A., corroborando que las mismas no han sido respetadas en todas sus partes, recomendando su utilización ya que si bien no ofrecen soluciones, marcan una estructura beneficiosa que permitirá

identificar las debilidades planteadas con respecto a la seguridad lógica informática de la Empresa.

1.2.4. Objetivos específicos

- Analizar la situación actual en cuanto a riesgos informáticos en el departamento.

- Plantear recomendaciones basándose en COBIT para una buena Administración de Riesgos en el departamento.

1.2.5. Estructura de Desglose del Trabajo

Descripción de los Procesos, Técnicas y Actividades realizadas para desarrollar el T.F.G.:

1. Recopilación y análisis de información sobre COBIT e ISO aplicado a riesgos informáticos.

2. Recopilación y análisis de las herramientas a utilizarse.

3. Relevamiento y análisis de Información sobre el departamento.

4. Recopilación y análisis de información sobre Riesgos Informáticos utilizando ISO 17799.

5. Análisis de los riesgos lógicos existentes utilizando Herramienta COBIT.

6. Control de Riesgos Informáticos.

7. Informe Final.

1.3. Gestión de Tiempos

1.3.1. Identificación de actividades realizadas

Actividad 1: Recopilación y análisis de información sobre COBIT e ISO aplicado a riesgos informáticos.

Actividad 2: Relevamiento y análisis de Información sobre el Departamento de Informática de AGUA DE LOS ANDES S.A.

Actividad 3: Recopilación y análisis de las herramientas a utilizarse.

Actividad 4: Recopilación y análisis de información sobre Riesgos Informáticos utilizando ISO 17799.

Actividad 5: Análisis de riesgos lógicos existentes utilizando Herramienta COBIT.

Actividad 6: Control de Riesgos Informáticos.

Actividad 7: Informe Final.

1.3.2. Secuencia de las actividades

2.- Marco Teórico

2.1. Fundamentación Teórica

2.1.1. Uso del Marco Referencial COBIT

IT Governance Institute (2007). Cobit 4.1., señala que:

> 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 participantes. 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 TI.
>
> 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

- Entendimiento compartido entre todos los participantes, con base en un lenguaje común

- Cumplimiento de los requerimientos COSO[1] para el ambiente de control de TI.

En la siguiente figura (Figura 3) se muestra el Marco de Trabajo General de COBIT, con el modelo de procesos de COBIT compuesto de cuatro dominios que contienen 34 procesos genéricos, administrando los recursos de TI para proporcionar información al negocio de acuerdo con los requerimientos del negocio y de gobierno.

[1] COSO: Comité de organizaciones patrocinadoras de la comisión Treadway Estándar aceptado a nivel internacional para el gobierno corporativo. FUENTE: Documento COBIT 4.1

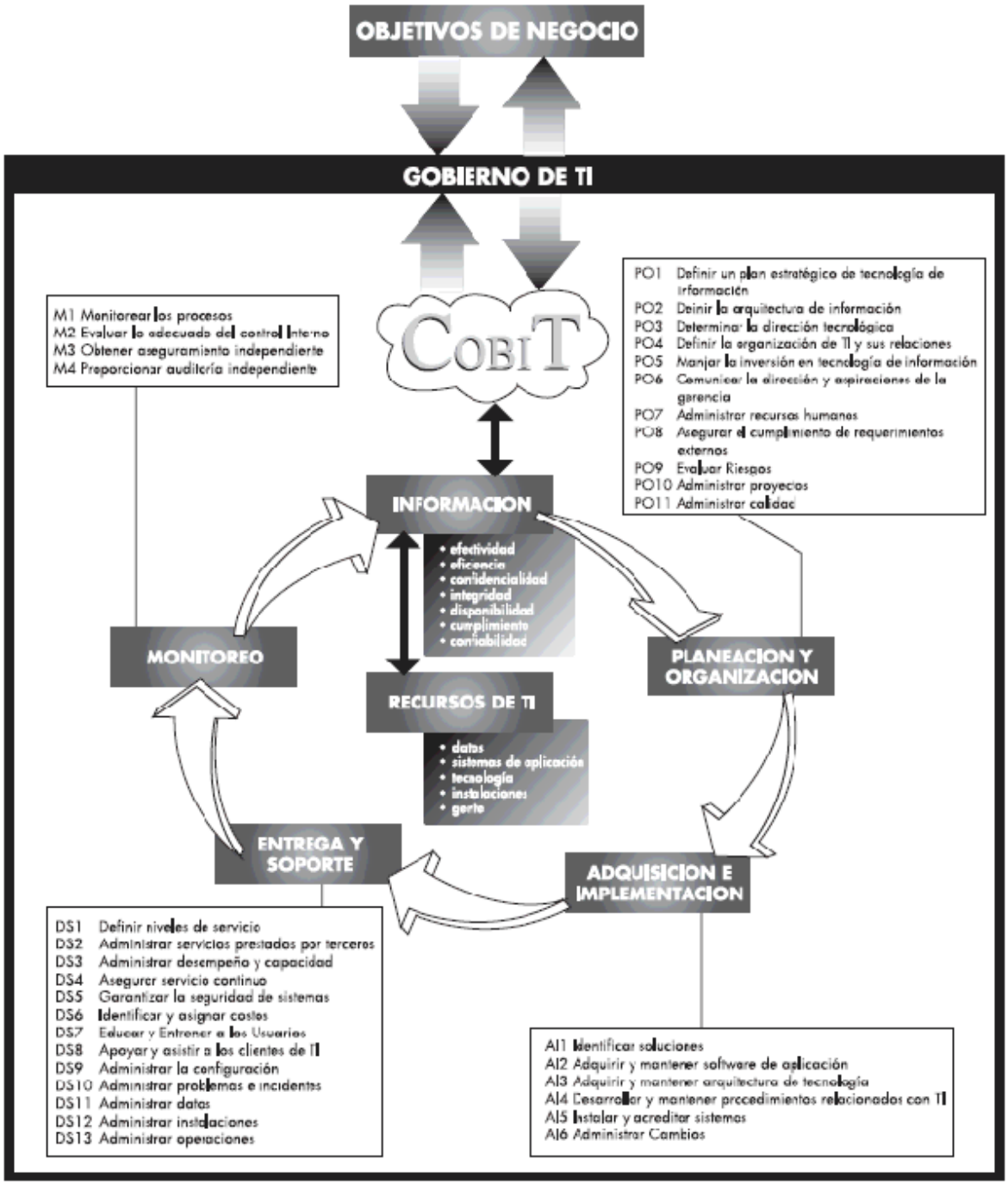

Figura 3: Marco de trabajo general de COBIT

2.1.2. Criterios de información de COBIT

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

- *Efectividad* tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.

- *Eficiencia* consiste en que la información sea generada optimizando los recursos (más productivo y económico).

- *Confidencialidad* se refiere a la protección de información sensitiva contra revelación no autorizada.

- *Integridad* está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.

- *Disponibilidad* se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne con la protección de los recursos y las capacidades necesarias asociadas.

- *Cumplimiento* tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.

- *Confiabilidad* significa proporcionar la información apropiada para que la gerencia administre la entidad y ejercite sus responsabilidades fiduciarias y de gobierno.

2.1.3. Recursos de TI

La organización de TI se desempeña con respecto a estas metas como un conjunto de procesos definidos con claridad que utiliza las habilidades de las personas, y la infraestructura de tecnología para ejecutar aplicaciones automatizadas de negocio, mientras que al mismo tiempo toma ventaja de la información del negocio.

Para responder a los requerimientos que el negocio tiene hacia TI, la empresa debe invertir en los recursos requeridos para crear una

capacidad técnica adecuada para dar soporte a la capacidad del negocio que genere el resultado deseado.

Los recursos de TI identificados en COBIT se pueden definir como sigue:

- *Aplicaciones* incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.

- *Información* son los datos en todas sus formas de entrada, procesados y generados por los sistemas de información, en cualquier forma en que son utilizados por el negocio.

- *Infraestructura* es la tecnología y las instalaciones (Sistemas operativos, sistemas de administración de base de datos, redes, multimedia, entre otras, así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.

- *Personas* son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

-

En la siguiente tabla (Tabla 2) se muestra el impacto de los objetivos de control COBIT sobre los recursos y criterios de TI. En los recursos de TI una X significa que ese objetivo de control tiene impacto sobre el recurso y un espacio en blanco que no tiene impacto. En los criterios de información se identifica el grado de impacto; Primario (P), para indicar impacto directo sobre el criterio de información, Secundario (S) impacto indirecto o en menor medida y espacio en blanco o vacío, que no tiene impacto alguno.

		Criterios de Información							**Recursos de TI**			
Dominio	Proceso	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Personas	Sistemas	Aplicación	Infraestructura
	Planeación y Organización											
PO1	Definir un Plan Estratégico de TI	P	S						X	X	X	X
PO2	Definir la Arquitectura de Información	S	P	S	P					X	X	
PO3	Definir la dirección tecnológica	P	P								X	X
PO4	Definir los Procesos, Organización y Relaciones de TI	P	P						X			
PO5	Administrar la Inversión en TI	P	P					S	X		X	X
PO6	Comunicar las metas y la dirección de la gerencia	P					S		X	X		
PO7	Administrar Recursos Humanos	P	P						X			
PO8	Administrar la Calidad	P	P		S			S	X	X	X	X
PO9	Evaluar y Administrar los Riesgos de TI	S	S	P	P	P	S	S	X	X	X	X

PO10	Administrar proyectos	P	P						X		X	X	
Adquisición e Implementación													
AI1	Identificar las Soluciones Automatizadas	P	S								X	X	
AI2	Adquisición y Mantener Software de Aplicación	P	P		S			S			X		
AI3	Adquirir y Mantener la Infraestructura Tecnológica	S	P		S	S						X	
AI4	Facilitar la operación y el uso	P	P		S	S	S	S	X		X	X	
AI5	Procurar Recursos de TI	S	P				S		X	X	X	X	
AI6	Administrar Cambios	P	P		P	P		S	X	X	X	X	
AI7	Instalar y Acreditar soluciones y cambios	P	S		S	S			X	X	X	X	
Servicios y Soporte													
DS1	Definir y Administrar los Niveles de Servicio	P	P	S	S	S	S	S	X	X	X	X	
DS2	Administrar Servicios de Terceros	P	P	S	S	S	S	S	X	X	X	X	
DS3	Administrar EL Desempeño y Capacidad	P	P			S					X	X	
DS4	Asegurar Servicio Continuo	P	S			P			X	X	X	X	
DS5	Garantizar la Seguridad de Sistemas			P	P	S	S	S	X	X	X	X	
DS6	Identifica y Asignar Costos		P					P	X	X	X	X	
DS7	Educar y Entrenar a los Usuarios	P	S						X				
DS8	Administrar la mesa de Servicio y los Incidentes	P	P						X		X		
DS9	Administrar la Configuración	P	S			S		S		X	X	X	
DS10	Administrar los Problemas	P	P			S			X	X	X	X	
DS11	Administrar Datos				P			P		X			
DS12	Administrar el Ambiente Físico				P	P						X	
DS13	Administrar Operaciones	P	P		S	S			X	X	X	X	

Monitoreo													
ME1	Monitorear y Evaluar el desempeño de TI	P	P	S	S	S	S	S	X	X	X	X
ME2	Monitorear y evaluar el Control Interno	P	P	S	S	S	S	S	X	X	X	X
ME3	Garantizar el cumplimiento Regulatorio						P	S	X	X	X	X
ME4	Proporcionar Gobierno de TI	P	P	S	S	S	S	S	X	X	X	X

Tabla 2: Objetivos de Control COBIT, impacto en recursos TI y criterios de información

2.1.4. Norma ISO 17799 – 2005

Este Estándar Internacional establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delineados en este Estándar Internacional proporcionan un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados.

Los objetivos de control y los controles de este estándar son diseñados para ser implementados para satisfacer los requerimientos identificados por una evaluación del riesgo. La norma puede servir como un lineamiento práctico para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas y para ayudar a elaborar la confianza en las actividades interorganizacionales.

2.1.5. Modelos de Madurez

Cada vez con más frecuencia, se les pide a los directivos de empresas corporativas y públicas que se considere qué tan bien se está administrando TI.

Como respuesta a esto, se debe desarrollar un plan de negocio para mejorar y alcanzar el nivel apropiado de administración y control sobre la infraestructura de información.

Puede resultar difícil proporcionar respuestas significativas a estas preguntas. La gerencia de TI está buscando constantemente herramientas de evaluación por benchmarking[2] y herramientas de auto-evaluación como respuesta a la necesidad de saber qué hacer de manera eficiente. Comenzando con los procesos y los objetivos de control de alto nivel de COBIT, el propietario del proceso se debe poder evaluar de forma progresiva, contra los objetivos de control.

Esto responde a tres necesidades:

1. Una medición relativa de dónde se encuentra la empresa
2. Una manera de decidir hacia dónde ir de forma eficiente
3. Una herramienta para medir el avance contra la meta

[2] Benchmarking: es una técnica utilizada para medir el rendimiento de un sistema o componente de un sistema, frecuentemente en comparación con el cual se refiere específicamente a la acción de ejecutar un benchmark. Fuente: http://es.wikipedia.org/wiki/Benchmark

El modelado de la madurez para la administración y el control de los procesos de TI se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente (Nivel 0) hasta un nivel de optimizado (Nivel 5). Este enfoque se deriva del modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad del desarrollo de software. Cualquiera que sea el modelo, las escalas no deben ser demasiado granulares, ya que eso haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable debido a que en general, el fin es identificar dónde se encuentran los problemas y cómo fijar prioridades para las mejoras. El propósito no es avaluar el nivel de adherencia a los objetivos de control.

Los niveles de madurez están diseñados como perfiles de procesos de TI que una empresa reconocería como descripciones de estados posibles actuales y futuros.

No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior. Si se usan los procesos de madurez desarrollados para cada uno de los 34 procesos TI de COBIT, la administración podrá identificar:

- El desempeño real de la empresa—Dónde se encuentra la empresa hoy
- El estatus actual de la industria—La comparación
- El objetivo de mejora de la empresa—Dónde desea estar la empresa

Se ha definido un modelo de madurez para cada uno de los 34 procesos de TI, con una escala de medición creciente a partir de 0, no existente, hasta 5, optimizado. El desarrollo se basó en las descripciones del modelo de madurez genérico descritas en la Tabla 3.

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.

Tabla 3: Modelo genérico de madurez

3. Ejecución del T.F.G.

La Empresa Agua de los Andes S.A. surge de la transformación de la Dirección Provincial de Agua Potable y Saneamiento de Jujuy, cuya vigencia se instrumenta mediante decreto N° 2091-E-95, del día 1° de Junio de 1995.

A través de esta nueva figura legal, la empresa Agua de los Andes S.A., brazo ejecutor de las políticas de saneamiento del Gobierno de la Provincia de Jujuy continúa desarrollando su accionar en dos tipos de servicios:

- Provisión de agua potable.
- Recolección y tratamiento de líquidos cloacales

Desde la transformación de la Dirección Provincial de Agua Potable y Saneamiento de Jujuy, la empresa ha experimentado transformaciones en algunos aspectos de seguridad; la situación actual da a conocer que los sistemas informáticos son el activo más valioso y al mismo tiempo el más vulnerable.

La finalidad de este trabajo es investigar el estado actual de la seguridad informática a través del uso de la norma ISO 17799 y COBIT.

Identificación de la Empresa

Nombre: AGUA DE LOS ANDES S.A.

Dirección: Calle Alvear N° 947 San Salvador de Jujuy.

Teléfono: 0800-444-26337

Estructura Organizacional

La estructura organizacional de Agua de los Andes S.A. está dividida en varios niveles en los cuales se encuentran tanto los órganos directivos como las diferentes gerencias.

En la siguiente figura (Figura 1) se muestra la estructura organizacional.

Figura 1: Estructura Organizacional de Agua de los Andes S.A.

Con esta estructura organizacional de Agua de los Andes S.A. podemos dar cuenta que el Área de Sistemas se encuentra bajo la Gerencia General ya que el área de sistemas da soporte a todos los departamentos de la empresa además de tener un poder de decisión más independiente que otros departamentos[3].

Estructura organizacional del Departamento de Informática[4]

La misión fundamental del Área de Sistemas es el diseño, implementación y mantenimiento de los elementos que constituyen la infraestructura informática de la Empresa, entendiendo por tal los elementos físicos, lógicos, configuraciones y procedimientos necesarios para proporcionar a toda la Empresa los servicios informáticos necesarios para desarrollar sus actividades.

El Departamento cuenta con ocho personas cuyos cargos se encuentran detallados en la Tabla 1.

CARGO	CANTIDAD DE PERSONAS
JEFE DE DEPARTAMENTO	1
SUPERVISOR	1
DISEÑADOR DE PAGINA WEB	1
DESARROLLADOR DE SOFTWARE	3
REPARADOR DE PC	1
ENCARGADO DE REDES	1

Tabla 1: Recurso Humano del Departamento de Informática

[3] Proporcionado por el Jefe del Departamento de Informática de AGUA DE LOS ANDES S.A
[4] Proporcionado por el Jefe del Departamento de Informática de AGUA DE LOS ANDES S.A

En la siguiente figura (Figura 2) se indica la estructura organizacional distribuida en el Departamento de Informática.

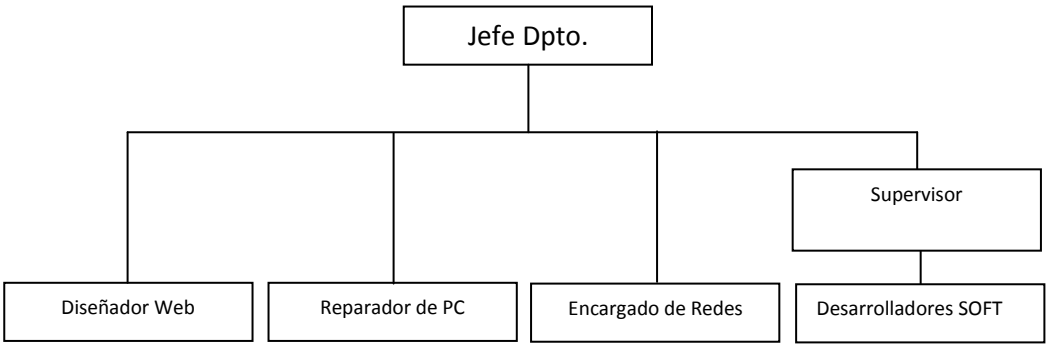

Figura 2: Estructura Organizacional del Departamento de Informática.

Diagrama Orgánico Funcional

De acuerdo a datos obtenidos por medio de entrevistas a los integrantes se enumera la distribución orgánica funcional del Departamento de Informática.

Jefe de Departamento

- Organización y administración del Departamento de Informática.

- Negociación con proveedores de Software, adquisición y evaluación de los mismos.

- Diseño y administración de la Base de Datos.

- Diseño y Administración de Redes.

- Reuniones con Gerencia para la presentación de Reportes y planificación de trabajo.

- Revisión de procedimientos del trabajo de sus dirigidos y reuniones semanales para la planificación del trabajo.

- Programación, Diseño e Implantación.

- Administración del Cableado de Red.

- Capacitación del personal según la necesidad.

Supervisor

- Supervisión y Administración de Servidores.

- Soporte a usuarios en general.

- Uso de software especializado en función de ciertas áreas.

- Soporte en Cableado estructurado.

- Análisis, diseño, implementación e implantación de sistemas de soporte a las necesidades de la empresa.

- Creación y administración de claves de acceso a aplicaciones.

- Asistencia técnica en la toma de decisiones para adquirir un nuevo producto o mantener los actuales.

Diseñador de Pagina Web[5]

- Desarrollo de Software en distintas plataformas como .NET, Oracle entre otras.

- Actualización del Sitio Web

[5] Empleado de Softlogía S.R.L. http://www.softlogia.com/ que trabaja exclusivamente para la empresa

Desarrollador de Software

- Desarrollo y administración de aplicativos en Genexus.
- Soporte a usuarios, mantenimiento y control de Software.
- Administración de perfiles de usuarios.
- Administración de Respaldos de la Base de Datos.
- Generación de Informes y Políticas de el Departamento de Informática.
- Actualización de datos de la Base de Datos.
- Esporádicamente ayuda en programación Web.

Reparador de PC

- Soporte Técnico a usuarios.
- Instalación de equipos.

- Mantenimiento de equipos (preventivo y correctivo).

- Cableado estructurado.

Encargado de Redes

- Diseño y Administración de Redes.

- Monitoreo y Reportes de Red.

- Cableado estructurado.

- Configuración de la red.

- Administración de perfiles de usuarios de red.

- Seguridad de redes.

Funciones del Departamento de Informática

A continuación se enumera las principales funciones:

- Desarrollar Aplicaciones utilizando herramientas de programación como Genexus, Punto Net, Java entre otras.

- Administrar los servidores de la empresa, realizar el monitoreo, respaldos y brindar el mantenimiento a los equipos y las aplicaciones (bases de datos, servidores Web, entre otros), así como también verificar los aspectos relacionados con seguridad.

- Administrar la Base de Datos; definir y controlar las bases de dato.

- Negociar compras de equipos informáticos.

3.1. Análisis de la Seguridad Lógica utilizando ISO/IECE 17799.

El Estándar Internacional ISO/IECE 17799 - 2005[6] (Ver *ANEXO 2*) contiene once cláusulas de control, cada cláusula contiene un número de categorías de seguridad principales:

- Política de Seguridad
- Organización de la Seguridad de la Información
- Gestión de Activos
- Seguridad de Recursos Humanos
- Seguridad Física y Ambiental
- Gestión de Comunicaciones y Operaciones
- Control de Acceso

[6] ANEXO 2: Estándar Internacional ISO/IEC 17799, Segunda Edición Junio 2005

- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

- Gestión de Incidentes de Seguridad de la Información

- Gestión de la Continuidad Comercial

- Conformidad

Se realizo un análisis acerca de la Seguridad Lógica en el Departamento de Informática de Agua de los Andes S.A. y el resultado se obtuvo siguiendo las clausulas de control mencionadas anteriormente, tomando la información de entrevistas realizadas al personal de la Empresa (*ANEXO* 3) y el relevamiento realizado dentro del departamento (*ANEXO 1*). Dicho resultado se detalla a continuación:

3.1.1. Política de Seguridad[7]

Política de Seguridad de la Información

- No cuenta con un Plan Estratégico de Seguridad.
- Existe un Plan Informático en borrador utilizado como agenda de actividades.
- No existe Plan de Contingencias.

[7] Proporcionado por el Jefe del Departamento de Informática de AGUA DE LOS ANDES S.A.

- La seguridad informática no está vista como un aspecto muy importante dentro de la Empresa.

- No existe un Plan de selección y presupuesto de las inversiones a realizar en Seguridad.
- No hay políticas y procedimientos formales respecto a la contratación con terceros. Los servicios de terceros no son ni aprobados ni revisados por la Gerencia. La Gerencia no está al tanto de la calidad del servicio prestado.
- No se controla debidamente la información.
- No hay reconocimiento de la necesidad de establecer un conjunto de políticas, procedimientos, estándares y procesos de cumplimiento.
- La organización carece de procedimientos para monitorear la efectividad de los controles internos.

3.1.2. Organización de la Seguridad de la Información

Organización Interna

- El Jefe del Departamento está consciente que se debe elaborar una Política de Seguridad y difundirla a los integrantes del área pero no se observa compromiso para realizarlo.

- No existe una estructura de gestión para iniciar y controlar la implantación de la seguridad de la información.

- Si bien están definidos claramente los roles y responsabilidades de cada empleado, todo es acuerdo verbal. Las tareas se realizan de acuerdo a las necesidades y conocimientos del personal.
- No existe ningún especialista en seguridad dentro de la Empresa.

- La Gerencia no reconoce la necesidad de contar con un programa de capacitación del personal.

Grupos o Personas Externas

- No se tiene contacto con especialistas expertos en seguridad para mantenerse al día en las tendencias de la industria, la evolución de las normas y métodos de evolución, así como tener un punto de enlace para tratar las incidencias de seguridad.

3.1.2. Gestión de Activos

Responsabilidades sobre los Activos

- Los inventarios de los activos que se tiene no están realizados con ningún tipo de formato especificado por normas de manejo de seguridad.

- No se tiene documentado ni implementadas reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información.

Clasificación de la Información

- Existen muchos tipos de activos que no se respaldan dentro del Departamento como:
    - Información: Información de investigaciones, manuales del usuario, material de capacitación, procedimientos operacionales o de soporte, rastros de auditoría e información archivada entre los mas destacados.

    - Activos de software: Software de aplicación, software del sistema, herramientas de desarrollo y utilidades.

3.1.3. Seguridad de Recursos Humanos

Antes del empleo.

- No siempre se define claramente el proceso de contratación de empleados con roles, responsabilidades, derechos y obligaciones.
- No siempre se realiza una verificación de antecedentes con la información que se registra en el CV.

Durante el desempeño de funciones.

- Si bien se tiene roles y responsabilidades definidos, todos realizan distintas actividades de acuerdo a las necesidades y conocimientos.
- De las entrevistas realizadas se deduce que en ciertas ocasiones todo el equipo realiza las mismas actividades es decir se desempeñan de acuerdo a las necesidades.
- No se tiene una adecuada capacitación con respecto a la seguridad de la información de la empresa, según la función laboral de cada empleado.

3.1.4. Seguridad Física y Ambiental

Áreas seguras

- Existen cámaras de seguridad instaladas en la entrada del departamento.
- Existe contratada vigilancia privada por medio de una compañía dedicada a este fin, la misma que tiene sus correspondientes políticas de contratación.

Equipo de seguridad

- El Sector cuenta con un extintor de fuego, alarma, generador de energía, UPS, entre los más destacados.
- En el cuarto de servidores existe aire acondicionado que posee un sensor de temperatura que se activa automáticamente en caso de condiciones anormales del ambiente, en el edificio no se posee alarma para detectar fuego, calor, humo o fugas de agua.

- El personal no está capacitado en caso de que suceda alguna emergencia, simplemente actuará por instinto o por lo que generalmente se conoce.
- Existen normas generales que no se cumplen para salvaguardar los equipos como:

    - No fumar dentro de las instalaciones.

    - No consumir alimentos dentro del cuarto de servidores.

- El cableado de la red no se tiene protegido mediante canaletas en el techo falso.

- No se tiene una política definida para cuando haya necesidad de sacar los equipos de las instalaciones ya sea por realizar trabajos en casa o por reparaciones fuera del edificio.

- Cuando existe la necesidad de retirar un equipo a un usuario no se tiene definido un procedimiento, solo se verifica las razones del cambio, se respalda la información necesaria y se procede a realizar el cambio actualizando en inventario.

3.1.5. Gestión de las Comunicaciones y Operaciones

Procedimientos y responsabilidades operacionales

- No se tiene un plan de procedimientos de operación de la información y de los equipos.
- Los procedimientos de operación no especifican las instrucciones para la ejecución detallada de cada trabajo como:

a) Procesamiento y manejo de información.

b) Copia de seguridad o respaldo.

c) Requerimientos de programación de horarios, incluyendo las interdependencias con otros sistemas, los tiempos de culminación y horarios de los primeros y últimos trabajos.

d) Instrucciones para el manejo de errores u otras condiciones excepcionales, las cuales podrían surgir durante la ejecución del trabajo, incluyendo las restricciones sobre el uso de las utilidades del sistema.

e) Contactos de soporte en el evento de dificultades operacionales o técnicas inesperadas.

f) Procedimientos de reinicio y recuperación del sistema para su uso en el evento de una falla en el sistema.

g) La gestión de la información del rastro de auditoría y registro del sistema.

Planeación y aceptación del sistema

- No se documentan ni prueban como corresponde los requerimientos operacionales de los sistemas nuevos antes de su aceptación y uso.
- No se tiene ni se realiza un monitoreo de los sistemas planificado, para evaluar el rendimiento del mismo.
- No se hace un estudio debidamente documentado para la aceptación de sistemas que vayan a ser usados.

Protección contra el código malicioso

- Se protege de los códigos maliciosos mediante el antivirus NOD32, no se tiene una política de revisión de virus en dispositivos móviles a ser ejecutados sino que se la realiza de manera informal; las personas que saben que deben revisar los dispositivos lo hacen, y los ejecutan de una manera que no afecte al sistema.

Respaldo o Back-Up

- Cuenta con una política de respaldos. Cada usuario está encargado de respaldar la información que utiliza y el Jefe de Departamento encargará a un miembro

respaldar el Sistema Operativo, Bases de Datos, y Aplicaciones, los mismos que los realizan en Discos duros y DVD, escogidos por costos y seguridad. Los respaldos se envían a otro establecimiento de la empresa.

Gestión de seguridad de la red

- El administrador de la red (Encargado de Redes) realiza controles de la misma en cuanto a flujos de datos, monitoreo y protección; sin embargo no se cuenta con controles documentados para realizar estas tareas.

Gestión de medios

- Se controlan los medios y se los protege físicamente de acuerdo a la responsabilidad de cada unos de los integrantes del área; es decir cada uno tiene a su cargo algún medio y es responsable de su estado.

Intercambio de información

- Para realizar el intercambio de la información no se tiene una política diseñada, sino que el Departamento tiene definido quien debe tener información para cada tarea específica, y cuando se trata de información confidencial se hace un registro de la persona a quien se entregó dicha información, para que quede constancia de haberla entregado.
- Para la transmisión de información dentro de Agua de los Andes S.A. se utiliza Microsoft Outlook, como gestor de correo electrónico, y de esta manera la

persona encargada controla a quien, cuando, y que información ha sido enviada y recibida.

- Para mantener la confidencialidad de la información se tiene restringido el uso de programas de mensajería como Windows Messenger, Yahoo Messenger, Skype, entre otros. No se tiene restringido el uso de celular dentro del Departamento lo que es un riesgo ya que se puede revelar información confidencial por este medio.

Monitoreo

- No existen procedimientos de monitoreo para asegurar que los usuarios sólo estén realizando actividades para las cuales han sido explícitamente autorizados.
- Para acceder a los sistemas se tiene perfiles definidos para cada uno de los usuarios, con estos controles se administra las fallas ocurridas en los sistemas para tomar acciones correctivas ante ellas.

3.1.6. Control de Acceso

Requerimiento del negocio para el control del acceso

- No cuenta con políticas para la divulgación, política de clasificación de la información y autorización de la información.
- No cuenta con una política de control de acceso lógico totalmente definida.

Gestión de acceso del usuario

- La manera como se asegura el acceso de usuarios autorizados y no autorizados a los sistemas de información es manejando perfiles, es decir login y passwords de acceso con sus respectivos permisos dentro de las aplicaciones.
- Existe una persona encargada de la administración de usuarios, desde el registro de usuarios nuevos hasta la terminación final del registro de los mismos que ya no requieren acceso a los sistemas y servicios de información; pero este no es un procedimiento estrictamente formal.
- El manejo de claves secretas no se controla a través de un proceso de gestión formal.

Responsabilidades del usuario

- El control de acceso de usuarios no autorizados para evitar poner en peligro la información y evitar el robo de la misma es manejado por cada uno de los miembros del departamento quienes tienen la responsabilidad de salvaguardar los equipos y la información que se encuentran a cargo.
- No existe una política de claves y contraseñas, el uso de las mismas es decidido por el usuario con consejo y consentimiento del personal de sistemas.

Control de acceso a la red

- El control de acceso a los servicios de redes lo realiza el administrador de la red o la persona encargada de esta función, no se tiene una política definida al

respecto pero se controla mediante interfaces apropiadas y mecanismos de autenticación.

- El control de acceso y configuración está a cargo del administrador de la red y el Jefe del Departamento.
- Se restringe: Correo electrónico, mensajería instantánea, transferencia de archivos y acceso a aplicaciones.
- En cuanto a controles de rutina no hay una reglamentación establecida ya que como se dijo anteriormente no existe una política de control de acceso.

Control del acceso al Sistema

- Para evitar el acceso no autorizado a los sistemas operativos se autentifica a los usuarios autorizados pero no se registra los intentos exitosos y fallidos de autenticación del sistema.
- No se restringe debidamente el tiempo de conexión de los usuarios.
- Las sesiones inactivas se bloquean después de un periodo de inactividad.

Control de acceso a la aplicación y la información

- Para evitar el acceso no autorizado a la información en los sistemas de aplicación no existe una política de control de acceso definida; sin embargo el control se lo realiza por medio de claves de acceso a usuarios autorizados los cuales tienen perfiles definidos, con sus respectivos privilegios de acuerdo a las funciones que necesite, en los sistemas de aplicación.

Computación y trabajo móvil

- Para garantizar la seguridad de la información cuando se utiliza medios de computación y trabajo móviles como notebooks el responsable del equipo debe tener especial cuidado.
- No hay una política de computación móvil claramente establecida pero como regla general se tiene precaución en cuanto a respaldos, control de acceso, protección física, conexiones inalámbricas y protección contra virus.

3.1.7. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

Requerimientos de seguridad de los sistemas de información

- En las aplicaciones que se desarrollan el Departamento define perfiles de usuario para manejar la seguridad de las mismas, así como también en las bases de datos de las aplicaciones.
- No se define requerimientos de seguridad pero se los maneja en los diferentes sistemas.

Procesamiento correcto en las aplicaciones

- Para prevenir errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones, se las realiza con las respectivas validaciones para el ingreso de información, y el procesamiento de dicha información es debidamente probado para evitar errores y riesgos de que se la use incorrectamente, se verifica que la salida de la información sea la que se

esperaba, mas sin embargo; la validación, verificación y pruebas; y la salida no siempre será la correcta; es decir, aún los sistemas que han sido probados pueden producir output incorrecto en algunas circunstancias. Por esta razón se debe implementar mejores prácticas para un mejor resultado.

Controles criptográficos

- Para proteger la confidencialidad, autenticidad e integridad a través de medios criptográficos. Se debe desarrollar una política sobre el uso de controles criptográficos.
- Se utilizan técnicas de criptografía que ofrecen los motores de bases de datos pero no se tienen definidas políticas en particular para manejarla.

Seguridad de los archivos del sistema

- Con el fin de garantizar la seguridad el almacenamiento de código fuente e instalación de software es solo gestionado por las personas asignadas por el Jefe del Departamento.

Seguridad en los procesos de desarrollo y soporte

- No se documentan y no se cumplen los procedimientos formales de control del cambio para minimizar errores de los sistemas de información, para probar los

cambios existe ambientes de prueba verificando que no comprometan a los procesos anteriores.

3.1.8. Gestión de un incidente en la Seguridad de la Información

Reporte de los eventos y debilidades de la seguridad de la información

- No tiene implementado una política de reporte de debilidades, sino que según sea el caso de emergencia se soluciona dichas eventualidades pero no con un procedimiento determinado, no se ha informado a los usuarios que se tome nota y se reporte cualquier debilidad de seguridad observada o sospechada en el sistema o los servicios.

Gestión de los incidentes y mejoras en la seguridad de la información

- No se tiene un registro de eventualidades que han sido solucionadas, para su monitoreo y procurar que no vuelvan a suceder.

3.1.9. Gestión de la continuidad del negocio

Aspectos de la seguridad de la información de la gestión de la continuidad del Negocio

- No existe un plan de contingencia donde se tome en cuenta aspectos de la seguridad de la información de la gestión de la continuidad del negocio.
- Para salvaguardar la información se implementa un plan de respaldos.

3.1.10. Cumplimiento

Cumplimiento de los requerimientos legales

- No todo el software cuenta con las licencias de uso respectivas y en regla.
- No se cuenta con una política apropiada con respecto al uso de licencias y que garantice los derechos de propiedad intelectual de los sistemas que se han implementado así como con una política de protección y privacidad de los datos.

Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico

- La seguridad de los sistemas de información se revisa cada vez que es requerido, es decir, cuando se detecta algún error debido a la falta de seguridad.
- El Jefe de Departamento verifica el cumplimiento de los procedimientos de seguridad dentro del área y en caso de un incumplimiento se pide rendición de cuentas a la persona encargada.
- La detección de vulnerabilidades en los sistemas lo hacen las personas del Departamento y también los usuarios finales.

Consideraciones de auditoría de los sistemas de información

- No se ha realizado auditoría de los sistemas de información, ni internamente ni externamente.

3.2. Implementación

3.2.1. Integración ISO/IECE 17799 - COBIT

En la siguiente tabla (Tabla 4) se integra los objetivos de control de COBIT y la norma ISO/IECE 17799-2005; basado en el documento COBIT SECURITY BASELINE, en el cual se mapea los objetivos de control de COBIT con las cláusulas de control de seguridad de la norma ISO. De esta manera se seleccionaran los objetivos de control concernientes a la evaluación de los riesgos fundamentándose en la norma.

CLAUSULAS NORMA ISO/IECE 17799	OBJETIVOS DE CONTROL COBIT DETALLADOS
1. Política de seguridad 1.1 Política de seguridad de la información	PO3.1, PO5.3, PO5.4, PO6.1, PO6.2, PO6.3, PO6.4, PO7.4, PO9.4, DS4.1, DS5.5, DS5.6, DS7.1, ME2.1, ME2.4
2. Organización de la Seguridad de la Información 2.1 Organización interna 2.2 Grupos o personas externas	PO1.3, PO1.4, PO1.5, PO2.3, PO3.1, PO3.3, PO4.3, PO4.4, PO4.5, PO4.6, PO4.8, PO4.9, PO4.10, PO4.14 , PO4.15, PO6.1, PO6.3,PO6.4, PO6.5, PO7.2, PO7.4, PO7.5, PO9.3 , PO9.4, PO10.4, AI1.2, AI1.3, AI2.1, AI2.3, AI3.1, AI3.2, AI3.3, AI5.2, AI5.6, AI6.1, AI6.3, AI7.12, AI7.6, AI7.8, DS2.1, DS2.2, DS2.3, DS2.4, DS4.1, DS4.3, DS5.1, DS5.1, DS5.3, DS5.4, DS5.5, DS5.6, DS5.11, DS7.2, DS10.1, DS10.2, DS11.6, DS12.1, DS12.3, ME2.1, ME2.2, ME2.3, ME2.4, ME2.5.
3. Gestión de Activos 3.1 Responsabilidades sobre los activos. 3.2 Clasificación de la Información	PO2.3, PO3.1, PO4.9, PO4.10, PO6.3, PO6.4, PO6.5, PO9.3, AI2.2, AI6.5, AI7.8, DS9.1, DS9.2, DS9.3, DS11.2, DS11.3, DS11.6, DS13.4, ME3.1.
4. Seguridad de Recursos Humanos 4.1 Antes del empleo. 4.2 Durante el desempeño de funciones.	PO4.6, PO4.8, PO4.14, PO6.1, PO6.3 PO6.4, PO6.5, PO7.1, PO7.2, PO7.4, PO7. , PO7.7, PO7.8, AI5.3, DS2.3, DS2.4, DS5.4, DS7.1, DS12.1.
5. Seguridad Física y Ambiental 5.1 Áreas seguras 5.2 Equipo de seguridad	PO4.14, PO6.3, PO6.4, PO6.5, PO9.3, AI6.3, AI7.11, DS4.1, DS4.7, DS4.8, DS4.9, DS5.3, DS5.4, DS5.7, DS9.3, DS10.2, DS11.4, DS12.1, DS12.2, DS12.3, DS12.4, DS12.5, DS13.2, DS13.5, ME3.1.
6. Gestión de las Comunicaciones y Operaciones 6.1 Procedimientos y responsabilidades operacionales 6.3 Planeación y aceptación del sistema 6.4 Protección contra el código malicioso y móvil 6.5 Respaldo o Back-Up 6.6 Gestión de seguridad de la red 6.7 Gestión de medios 6.8 Intercambio de información 6.10 Monitoreo	PO2.3, PO3.1, PO3.4, PO3.5, PO4.6, PO4.11, PO6.3, PO6.4, PO6.5, PO7.4, PO7.5, AI1.1, AI2.1, AI2.2, AI2.3, AI2.8, AI3.1, AI3.2, AI3.4, AI4.2, AI4.3, AI4.4, AI5.2, AI5.6, AI6.1, AI6.2, AI6.3, AI7.1, AI7.4, AI7.6, AI7.8, DS2.3, DS3.1, DS3.2, DS3.3, DS3.4, DS3.5, DS4.1, DS4.9, DS5.3, DS5.4, DS5.5, DS5.6, DS5.10, DS5.11, DS9.1, DS9.3, DS10.1, DS10.2, DS10.3, DS10.4, DS11.2, DS11.3, DS11.4, DS11.5, DS11.6, DS12.1, DS12.2, DS12.3, DS12.5, DS13.1, DS13.2, DS13.4, ME2.1, ME2.2, ME2.3, ME2.4, ME3.1.

7. Control de Acceso 7.1 Requerimiento del negocio para el control del acceso 7.2 Gestión de acceso del usuario 7.3 Responsabilidades del usuario 7.4 Control de acceso a la red 7.5 Control del acceso al sistema operativo 7.6 Control de acceso a la aplicación y la información. 7.7 Computación y tele-trabajo móvil	PO2.3, PO3.4, PO3.5, PO6.3, PO6.4, PO6.5, PO7.4, PO7.5, PO7.8, PO9.3, AI1.1, AI1.2, AI3.1, AI3.2, AI6.3, DS4.1, DS5.3, DS5.4, DS5.5, DS5.6, S5.11, DS7.1, DS12.1, DS12.2, DS12.3.
8. Adquisición Desarrollo y Mantenimiento de los Sistemas de Información 8.1 Requerimientos de seguridad de los sistemas de información 8.2 Procesamiento correcto en las aplicaciones 8.3 Controles criptográficos 8.4 Seguridad de los archivos del sistema 8.5 Seguridad en los procesos de desarrollo y soporte	PO2.1, PO2.3, PO6.3, PO6.4, PO6.5, PO9.3, PO9.5, AI1.1, AI1.2, AI2.2, AI2.3, AI2.4, AI2.8, AI3.1, AI3.3, AI3.4, AI5.1, AI5.2, AI5.3, AI5.4, AI5.5, AI6.1, AI6.2, AI6.3, AI6.4, AI6.5, AI7.10, AI7.11, AI7.6, DS2.3, DS2.4, DS4.1, DS5.3, DS5.4, DS5.7, DS5.8, DS5.11, DS9.1, DS9.2, DS11.5, DS11.6, ME3.1.
9. Gestión de un incidente en la Seguridad de la Información 9.1 Reporte de los eventos y debilidades de la seguridad de la Información 9.2 Gestión de los incidentes y mejoras en la seguridad de la información	PO5.3, PO6.1, PO6.2, PO6.3, PO6.4, PO6.5, PO7.4, AI1.1, AI4.3, AI4.4, AI6.1, AI6.5, AI7.11, DS2.3, DS3.5, DS5.5, DS5.6, DS5.9, DS8.1, DS8.3, DS8.5, DS10.1, DS10.2, DS10.3, DS10.4, DS13.2, ME2.1, ME2.2, ME2.3, ME2.4.
10. Gestión de la Continuidad del Negocio 10.1 Aspectos de la seguridad de la información de la gestión de la continuidad del Negocio	PO3.1, PO7.5, AI1.1, AI1.2, AI6.5, DS2.1, DS4.1, DS4.2, DS4.3, DS4.4, DS4.5, DS4.6, DS4.8, DS10.1, DS8.3, DS10.2.
11. Cumplimiento 11.1 Cumplimiento de los requerimientos legales 11.2 Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico 11.3 Consideraciones de auditoría de los sistemas de información	PO2.3, PO4.8, PO4.14, PO6.2, PO6.3, PO6.4, PO6.5, PO7.4, AI1.1, AI1.2, AI3.2, DS4.9, DS5.1, DS5.5, DS9.3, DS11.2, DS11.3, DS11.4, DS13.4, ME1.2, ME2.2, ME2.4, ME2.5, M3.1, M3.2, M3.7.

Tabla 4: Mapeo ISO 17799 y COBIT

3.2.2. Determinación de los procesos COBIT aplicables.

La determinación de los procesos COBIT involucrados para realizar el trabajo de Riesgos Informáticos en el Departamento de Informática de Agua de los Andes S.A., fue realizada según el mapeo de los mismos con las normas ISO descritas anteriormente, los cuales se evaluarán estableciendo el grado de madurez de los procesos organizacionales. Dichos procesos se muestran a continuación (Tabla 5)

PLANEAR Y ORGANIZAR	
PO1	Definir el Plan Estratégico de TI
PO2	Definir la Arquitectura de la Información
PO3	Determinar la dirección tecnológica
PO4	Definir procesos, organización y relaciones de TI.
PO5	Administrar la inversión en TI.
PO6	Comunicar las aspiraciones y la dirección de la gerencia
PO7	Administrar recursos humanos de TI
PO9	Evaluar y Administrar Riesgos de TI
PO10	Administrar proyectos
ADQUIRIR E IMPLEMENTAR	
AI1	Identificar Soluciones Automatizadas
AI2	Adquirir y mantener el software aplicativo
AI3	Adquirir y mantener la infraestructura tecnológica
AI4	Facilitar la operación y el uso
AI5	Adquirir recursos de TI
AI6	Administrar cambios
AI7	Instalar y Acreditar soluciones y cambios
ENTREGAR Y DAR SOPORTE	
DS2	Administrar servicios de terceros
DS3	Administrar desempeño y capacidad
DS4	Garantizar la Continuidad del Servicio
DS5	Garantizar la Seguridad de los Sistemas
DS7	Educar y entrenar a los usuarios
DS8	Administrar la mesa de servicio y los incidentes
DS9	Administrar la configuración
DS10	Administrar los problemas
DS11	Administrar los datos
DS12	Administrar el ambiente físico
DS13	Administrar las operaciones
MONITOREAR Y EVALUAR	
ME1	Monitorear y evaluar el Desempeño de TI
ME2	Monitorear y evaluar el control interno
ME3	Garantizar cumplimiento regulatorio

Tabla 5: Procesos aplicables al trabajo

3.2.3. Puesta en marcha del Control de Seguridad

En la siguiente tabla (Tabla 6) se muestra los objetivos de control escogidos para realizar el control y su impacto a los criterios de información y recursos de TI; la explicación de la misma ya se la realizó anteriormente.

		Criterios de Información							Recursos de TI			
Dominio	Proceso	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Personas	Sistemas	Aplicación	Infraestructura
Planeación y Organización												
PO1	Definir un Plan Estratégico de TI	P	S						X	X	X	X
PO2	Definir la Arquitectura de Información	S	P	S	P					X	X	
PO3	Definir la dirección tecnológica	P	P								X	X
PO4	Definir los Procesos, Organización y Relaciones de TI	P	P						X			
PO5	Administrar la Inversión en TI	P	P					S	X		X	X
PO6	Comunicar las metas y la dirección de la gerencia	P					S		X	X		
PO7	Administrar Recursos Humanos	P	P						X			
PO9	Evaluar y Administrar los Riesgos de TI	S	S	P	P	P	S	S	X	X	X	X
PO10	Administrar proyectos	P	P						X		X	X
Adquisición e Implementación												
AI1	Identificar las Soluciones Automatizadas	P	S								X	X
AI2	Adquisición y Mantener Software de Aplicación	P	P		S			S			X	
AI3	Adquirir y Mantener la Infraestructura Tecnológica	S	P		S	S						X
AI4	Facilitar la operación y el uso	P	P		S	S	S	S	X		X	X
AI5	Procurar Recursos de TI	S	P				S		X	X	X	X
AI6	Administrar Cambios	P	P		P	P		S	X	X	X	X
AI7	Instalar y Acreditar soluciones y cambios	P	S		S	S			X	X	X	X

Servicios y Soporte														
DS2	Administrar Servicios de Terceros	P	P	S	S	S	S	S		X	X	X	X	
DS3	Administrar EL Desempeño y Capacidad	P	P			S						X	X	
DS4	Asegurar Servicio Continuo	P	S			P				X	X	X	X	
DS5	Garantizar la Seguridad de Sistemas			P	P	S	S	S		X	X	X	X	
DS7	Educar y Entrenar a los Usuarios	P	S							X				
DS8	Administrar la mesa de Servicio y los Incidentes	P	P							X		X		
DS9	Administrar la Configuración	P	S			S		S			X	X	X	
DS10	Administrar los Problemas	P	P			S				X	X	X	X	
DS11	Administrar Datos				P			P			X			
DS12	Administrar el Ambiente Físico				P	P							X	
DS13	Administrar Operaciones	P	P		S	S				X	X	X	X	
Monitoreo														
ME1	Monitorear y Evaluar el desempeño de TI	P	P	S	S	S	S	S		X	X	X	X	
ME2	Monitorear y evaluar el Control Interno	P	P	S	S	S	S	S		X	X	X	X	
ME3	Garantizar el cumplimiento Regulatorio						P	S		X	X	X	X	

Tabla 6: Impacto de los objetivos de control a aplicarse

Fuente: Realizado por el autor

Para obtener los porcentajes de los criterios de información se asigna un valor al grado de impacto primario, secundario y blanco.

Para el análisis de resultados se toma como referencia el cuadro de interpretación (Tabla 7) según COSO[8] en cuanto al Nivel de Riesgo:

Calificación (%)		Grado de Confianza	Nivel de Riesgo
15%	50%	Bajo	Alto
51%	75%	Moderado	Moderado
76%	95%	Alto	Bajo
-	-	Vacío	Vacío

Tabla 7: Cuadro de Interpretación

Se genera una tabla de ponderación con el promedio de la calificación (Tabla 8) según la propuesta de COSO, con lo que se asigna un valor numérico al impacto de los criterios de información de cada proceso:

Nivel de Riesgo	Promedio	Grado de Confianza
Alto	32%	Bajo
Moderado	63%	Moderado
Bajo	86%	Alto

Tabla 8: Promedio de Nivel de Riesgo

Se coloca los valores propuestos en los criterios de Información que establece COBIT, dentro de cada uno de los procesos, utilizando la Tabla 7, especificando una calificación, como se puede ver en la Tabla 8; para el grado Primario se asigna el 86%, cuyo impacto es alto pero su nivel de riesgo es bajo; para el grado Secundario se asigna el 63% cuyo impacto y nivel de riesgo es moderado; y para el caso vacío no se asigna ningún valor, ya que no impacta a los criterios de información y no tiene nivel de riesgo.

[8] Sponsoring Organizations of the Treadway Commision.

OBJETIVOS DE CONTROL COBIT		Criterios de información de COBIT						
PLANEAR Y ORGANIZAR		**EFECTIVIDAD**	**EFICIENCIA**	**CONFIDENCIALIDAD**	**INTEGRIDAD**	**DISPONIBILIDAD**	**CUMPLIMIENTO**	**CONFIABILIDAD**
PO1	Definir un plan estratégico de TI	0,86	0,63					
PO2	Definir la Arquitectura de la Información	0,63	0,86	0,63	0,86			
PO3	Definir la dirección tecnológica	0,86	0,86					
PO4	Definir los Procesos	0,86	0,86					
PO5	Administrar la Inversión en TI	0,86	0,86					0,63
PO6	Comunicar las metas y la dirección de la gerencia	0,86					0,63	
PO7	Administrar los Recursos Humanos de TI	0,86	0,86					
PO9	Evaluar y Administrar los Riesgos de TI	0,63	0,63	0,86	0,86	0,86	0,63	0,63
PO10	Administrar los proyectos	0,86	0,86					
ADQUIRIR E IMPLANTAR								
AI1	Identificar las Soluciones Automatizadas	0,86	0,63					
AI2	Adquirir y Mantener Software Aplicativo	0,86	0,86		0,63			0,63
AI3	Adquirir y Mantener la Infraestructura Tecnológica	0,63	0,86		0,63	0,63		
AI4	Facilitar la operación y el uso	0,86	0,86		0,63	0,63	0,63	0,63
AI5	Procurar Recursos de TI	0,63	0,86				0,63	
AI6	Administrar los Cambios	0,86	0,86		0,86	0,86		0,63
AI7	Instalar y Acreditar soluciones y cambios	0,86	0,63		0,63	0,63		
ENTREGAR Y DAR SOPORTE								
DS2	Administrar los Servicios de Terceros	0,86	0,86	0,63	0,63	0,63	0,63	0,63
DS3	Administrar el Desempeño y la Capacidad	0,86	0,86			0,63		
DS4	Asegurar el Servicio Continuo	0,86	0,63			0,86		
DS5	Garantizar la Seguridad de los Sistemas			0,86	0,86	0,63	0,63	0,63
DS7	Educar y Entrenar a los Usuarios	0,86	0,63					
DS8	Administrar la mesa de Servicio y los Incidentes	0,86	0,86					
DS9	Administrar la Configuración	0,86	0,63			0,63		0,63
DS10	Administrar los Problemas	0,86	0,86			0,63		
DS11	Administrar los Datos				0,86			0,86
DS12	Administrar el Ambiente Físico				0,86	0,86		
DS13	Administrar las Operaciones	0,86	0,86		0,63	0,63		
MONITOREAR Y EVALUAR								
ME1	Monitorear y evaluar el desempeño de TI	0,86	0,86	0,63	0,63	0,63	0,63	0,63
ME2	Monitorear y evaluar el Control Interno	0,86	0,86	0,63	0,63	0,63	0,63	0,63
ME3	Garantizar el cumplimiento Regulatorio						0,86	0,63

Tabla 9: Resultados finales del impacto de los criterios de información

3.2.4. Modelos de madurez de los procesos

Se procede a la elaboración de cada una de las tablas de los modelos de madurez (Tabla 10 a Tabla 39), tomando en cuenta la situación del Departamento estudiada con la Norma ISO 17799 y luego respectivamente mapeado con COBIT; indicando con ello el grado de madurez y objetivos no cumplidos en cada uno de los procesos que establece COBIT.

DOMINIO: PLANEAR Y ORGANIZAR **PO1: Definir el plan estratégico de TI**			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	
0 No existente cuando No se lleva a cabo la planeación estratégica de TI. No existe conciencia por parte de la gerencia de que la planeación estratégica de TI es requerida para dar soporte a las metas del negocio.	**X**		**GRADO DE MADUREZ.** El proceso de definir el plan estratégico de TI se encuentra en el nivel 3
1 Inicial/Ad Hoc cuando La gerencia de TI conoce la necesidad de una planeación estratégica de TI. La planeación de TI se realiza según se necesite como respuesta a un requisito de negocio específico. La planeación estratégica de TI se discute de forma ocasional en las reuniones de la gerencia de TI. La alineación de los requerimientos de las aplicaciones y tecnología del negocio se lleva a cabo de modo reactivo en lugar de hacerlo por medio de una estrategia organizacional. La posición de riesgo estratégico se identifica de manera informal proyecto por proyecto.	**X**		
2 Repetible pero intuitiva cuando La planeación estratégica de TI se comparte con la gerencia del negocio según se necesite. La actualización de los planes de TI ocurre como respuesta a las solicitudes de la dirección. Las decisiones estratégicas se toman proyecto por proyecto, sin ser consistentes con una estrategia global de la organización. Los riesgos y beneficios al usuario, resultado de decisiones estratégicas importantes se reconocen de forma intuitiva.	**X**		
3 Proceso definido cuando Una política define cómo y cuándo realizar la planeación estratégica de TI. La planeación estratégica de TI sigue un enfoque estructurado, el cual se documenta y se da a conocer a todo el equipo. El proceso de planeación de TI es razonablemente sólido y garantiza que es factible realizar una planeación adecuada. Sin embargo, se otorga discrecionalidad a gerentes individuales específicos con respecto a la implantación del proceso, y no existen procedimientos para analizar el proceso. La estrategia general de TI incluye una definición consistente de los riesgos que la organización está dispuesta a tomar como innovador o como seguidor. Las estrategias de recursos humanos, técnicos y financieros de TI influencian cada vez más la adquisición de nuevos productos y tecnologías. La planeación estratégica de TI se discute en reuniones de la dirección del negocio.		**X**	
4 Administrado y medible cuando		**X**	

La planeación estratégica de TI es una práctica estándar y las excepciones son advertidas por la dirección. La planeación estratégica de TI es una función administrativa definida con responsabilidades de alto nivel. La dirección puede monitorear el proceso estratégico de TI, tomar decisiones informadas con base en el plan y medir su efectividad. La planeación de TI de corto y largo plazo sucede y se distribuye en forma de cascada hacia la organización, y las actualizaciones se realizan según son necesarias. La estrategia de TI y la estrategia organizacional se vuelven cada vez más coordinadas al abordar procesos de negocio y capacidades de valor agregado y al aprovechar el uso de aplicaciones y tecnologías por medio de la re-ingeniería de procesos de negocio. Existen procesos bien definidos para determinar el uso de recursos internos y externos requeridos en el desarrollo y las operaciones de los sistemas.			
5 Optimizado cuando La planeación estratégica de TI es un proceso documentado y vivo, que cada vez más se toma en cuenta en el establecimiento de las metas del negocio y da como resultado un valor observable de negocios por medio de las inversiones en TI. Las consideraciones de riesgo y de valor agregado se actualizan de modo constante en el proceso de planeación estratégica de TI. Se desarrollan planes realistas a largo plazo de TI y se actualizan de manera constante para reflejar los cambiantes avances tecnológicos y el progreso relacionado al negocio. Se realizan evaluaciones por comparación contra normas industriales bien entendidas y confiables y se integran con el proceso de formulación de la estrategia. El plan estratégico incluye cómo los nuevos avances tecnológicos pueden impulsar creación de nuevas capacidades de negocio y mejorar la ventaja competitiva de la organización.		**X**	

Tabla 10: MODELOS DE MADUREZ PO1

Fuente: Realizado por el autor

DOMINIO: PLANEAR Y ORGANIZAR **PO2: Definir la arquitectura de la información**			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de definir la arquitectura de la información se encuentra en el nivel 2
0 No existente cuando No existe conciencia de la importancia de la arquitectura de la información para la organización. El conocimiento, la experiencia y las responsabilidades necesarias para desarrollar esta arquitectura no existen en la organización.	**X**		
1 Inicial/Ad Hoc cuando La gerencia reconoce la necesidad de una arquitectura de información. El desarrollo de algunos componentes de una arquitectura de información ocurre de manera ad hoc. Las definiciones abarcan datos en lugar de información, y son impulsadas por ofertas de proveedores de software aplicativo. Existe una comunicación esporádica e inconsistente de la necesidad de una arquitectura de información.	**X**		
2 Repetible pero intuitiva cuando Surge un proceso de arquitectura de información y existen procedimientos similares, aunque intuitivos e informales, que se siguen por distintos individuos dentro de la organización. Las personas obtienen sus habilidades al construir la arquitectura de información por medio de experiencia práctica y la aplicación repetida de técnicas. Los requerimientos tácticos impulsan el desarrollo de los componentes de la arquitectura de la información por parte de los individuos.		**X**	
3 Proceso definido cuando La importancia de la arquitectura de la información se entiende y se acepta, y la		**X**	

responsabilidad de su aplicación se asigna y se comunica de forma clara. Los procedimientos, herramientas y técnicas relacionados, aunque no son sofisticados, se han estandarizado y documentado y son parte de actividades informales de entrenamiento. Se han desarrollado políticas básicas de arquitectura de información, incluyendo algunos requerimientos estratégicos, aunque el cumplimiento de políticas, estándares y herramientas no se refuerza de manera consistente. Existe una función de administración de datos definida formalmente, que establece estándares para toda la organización, y empieza a reportar sobre la aplicación y uso de la arquitectura de la información. Las herramientas automatizadas se empiezan a utilizar, aunque los procesos y reglas son definidos por los proveedores de software de bases de datos. Se definen, documentan y aplican actividades formales de entrenamiento de manera formal.			
4 Administrado y medible cuando Se da soporte completo al desarrollo e implantación de la arquitectura de información por medio de métodos y técnicas formales. La responsabilidad sobre el desempeño del proceso del desarrollo de la arquitectura se refuerza y se mide el éxito de la arquitectura de información. Las herramientas automatizadas de soporte están ampliamente generalizadas, pero todavía no están integradas. Se han identificado métricas básicas y existe un sistema de medición. El proceso de definición de la arquitectura de información es pro-activo y se enfoca en resolver necesidades futuras del negocio. La organización de administración de datos está activamente involucrada en todos los esfuerzos de desarrollo de las aplicaciones, para garantizar la consistencia. Un repositorio automatizado está totalmente implantado. Se encuentran en implantación modelos de datos más complejos para aprovechar el contenido informativo de las bases de datos. Los sistemas de información ejecutiva y los sistemas de soporte a la toma de decisiones aprovechan la información existente.		**X**	
5 Optimizado cuando La arquitectura de información es reforzada de forma consistente a todos los niveles. El valor de la arquitectura de la información para el negocio se enfatiza de forma continua. El personal de TI cuenta con la experiencia y las habilidades necesarias para desarrollar y dar mantenimiento a una arquitectura de información robusta y sensible que refleje todos los requerimientos del negocio. La información provista por la arquitectura se aplica de modo consistente y amplio. Se hace un uso amplio de las mejores prácticas de la industria en el desarrollo y mantenimiento de la arquitectura de información incluyendo un proceso de mejora continua. La estrategia para el aprovechamiento de la información por medio de un almacén de datos y tecnologías de minería de datos está bien definida. La arquitectura de la información se encuentra en mejora continua y toma en cuenta información no tradicional sobre los procesos, organizaciones y sistemas.		**X**	

Tabla 11: MODELOS DE MADUREZ PO2

Fuente: Realizado por el autor

DOMINIO: PLANEAR Y ORGANIZAR **PO3: Determinar la dirección tecnológica**			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de determinar la dirección tecnológica se encuentra en el nivel 3
0 No existente cuando No existe conciencia sobre la importancia de la planeación de la infraestructura tecnológica para la entidad. El conocimiento y la experiencia necesarios para desarrollar dicho plan de infraestructura tecnológica no existen. Hay una carencia de entendimiento de que la planeación del cambio tecnológico es crítica para asignar recursos de manera efectiva.	**X**		
1 Inicial/Ad Hoc cuando La gerencia reconoce la necesidad de planear la infraestructura tecnológica. El desarrollo	**X**		

de componentes tecnológicos y la implantación de tecnologías emergentes son ad hoc y aisladas. Existe un enfoque reactivo y con foco operativo hacia la planeación de la infraestructura. La dirección tecnológica está impulsada por los planes evolutivos, con frecuencia contradictorios, del hardware, del software de sistemas y de los proveedores de software aplicativo. La comunicación del impacto potencial de los cambios en la tecnología es inconsistente.			
2 Repetible pero intuitiva cuando Se difunde la necesidad e importancia de la planeación tecnológica. La planeación es táctica y se enfoca en generar soluciones técnicas a problemas técnicos, en lugar de usar la tecnología para satisfacer las necesidades del negocio. La evaluación de los cambios tecnológicos se delega a individuos que siguen procesos intuitivos, aunque similares. Las personas obtienen sus habilidades sobre planeación tecnológica a través de un aprendizaje práctico y de una aplicación repetida de las técnicas. Están surgiendo técnicas y estándares comunes para el desarrollo de componentes de la infraestructura.	**X**		
3 Proceso definido cuando La gerencia está consciente de la importancia del plan de infraestructura tecnológica. El proceso para el plan de infraestructura tecnológica es razonablemente sólido y está alineado con el plan estratégico de TI. Existe un plan de infraestructura tecnológica definido, documentado y bien difundido, aunque se aplica de forma inconsistente. La orientación de la infraestructura tecnológica incluye el entendimiento de dónde la empresa desea ser líder y dónde desea rezagarse respecto al uso de tecnología, con base en los riesgos y en la alineación con la estrategia organizacional. Los proveedores clave se seleccionan con base en su entendimiento de la tecnología a largo plazo y de los planes de desarrollo de productos, de forma consistente con la dirección de la organización.		**X**	
4 Administrado y medible cuando La dirección garantiza el desarrollo del plan de infraestructura tecnológica. El equipo de TI cuenta con la experiencia y las habilidades necesarias para desarrollar un plan de infraestructura tecnológica. El impacto potencial de las tecnologías cambiantes y emergentes se toma en cuenta. La dirección puede identificar las desviaciones respecto al plan y anticipar los problemas. La responsabilidad del desarrollo y mantenimiento del plan de infraestructura tecnológica ha sido asignado. El proceso para desarrollar el plan de infraestructura tecnológica es sofisticado y sensible a los cambios. Se han incluido buenas prácticas internas en el proceso. La estrategia de recursos humanos está alineada con la dirección tecnológica, para garantizar que el equipo de TI pueda administrar los cambios tecnológicos. Los planes de migración para la introducción de nuevas tecnologías están definidos. Los recursos externos y las asociaciones se aprovechan para tener acceso a la experiencia y a las habilidades necesarias. La dirección ha evaluado la aceptación del riesgo de usar la tecnología como líder, o rezagarse en su uso, para desarrollar nuevas oportunidades de negocio o eficiencias operativas.		**X**	
5 Optimizado cuando Existe una función de investigación que revisa las tecnologías emergentes y evolutivas y para evaluar la organización por comparación contra las normas industriales. La dirección del plan de infraestructura tecnológica está impulsada por los estándares y avances industriales e internacionales, en lugar de estar orientada por los proveedores de tecnología. El impacto potencial de los cambios tecnológicos sobre el negocio se revisa al nivel de la alta dirección. Existe una aprobación ejecutiva formal para el cambio de la dirección tecnológica o para adoptar una nueva. La entidad cuenta con un plan robusto de infraestructura tecnológica que refleja los requerimientos del negocio, es sensible a los cambios en el ambiente del negocio y puede reflejar los cambios en éste. Existe un proceso continuo y reforzado para mejorar el plan de infraestructura tecnológica. Las mejores prácticas de la industria se usan de forma amplia para determinar la dirección técnica.		**X**	

Tabla 12: MODELOS DE MADUREZ PO3

Fuente: Realizado por el autor

DOMINIO: PLANEAR Y ORGANIZAR PO4: Definir procesos, organización y relaciones de TI			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de definir el plan estratégico de TI se encuentra en el nivel 3
0 No existente cuando La organización de TI no está establecida de forma efectiva para enfocarse en el logro de los objetivos del negocio.	**X**		
1 Inicial/Ad Hoc cuando Las actividades y funciones de TI son reactivas y se implantan de forma inconsistente. IT se involucra en los proyectos solamente en las etapas finales. La función de TI se considera como una función de soporte, sin una perspectiva organizacional general. Existe un entendimiento explícito de la necesidad de una organización de TI; sin embargo, los roles y las responsabilidades no están formalizadas ni reforzadas.	**X**		
2 Repetible pero intuitiva cuando La función de TI está organizada para responder de forma táctica aunque de forma inconsistente, a las necesidades de los clientes y a las relaciones con los proveedores. La necesidad de contar con una organización estructurada y una administración de proveedores se comunica, pero las decisiones todavía dependen del conocimiento y habilidades de individuos clave. Surgen técnicas comunes para administrar la organización de TI y las relaciones con los proveedores.	**X**		
3 Proceso definido cuando Existen roles y responsabilidades definidos para la organización de TI y para terceros. La organización de TI se desarrolla, documenta, comunica y se alinea con la estrategia de TI. Se define el ambiente de control interno. Se formulan las relaciones con terceros, incluyendo los comités de dirección, auditoría interna y administración de proveedores. La organización de TI está funcionalmente completa. Existen definiciones de las funciones a ser realizadas por parte del personal de TI y las que deben realizar los usuarios. Los requerimientos esenciales de personal de TI y experiencia están definidos y satisfechos. Existe una definición formal de las relaciones con los usuarios y con terceros. La división de roles y responsabilidades está definida e implantada.		**X**	
4 Administrado y medible cuando La organización de TI responde de forma pro-activa al cambio e incluye todos los roles necesarios para satisfacer los requerimientos del negocio. La administración, la propiedad de procesos, la delegación y la responsabilidad de TI están definidas y balanceadas. Se han aplicado buenas prácticas internas en la organización de las funciones de TI. La gerencia de TI cuenta con la experiencia y habilidades apropiadas para definir, implantar y monitorear la organización deseada y las relaciones. Las métricas medibles para dar soporte a los objetivos del negocio y los factores críticos de éxito definidos por el usuario siguen un estándar. Existen inventarios de habilidades para apoyar al personal de los proyectos y el desarrollo profesional. El equilibrio entre las habilidades y los recursos disponibles internamente, y los que se requieren de organizaciones externas están definidos y reforzados. La estructura organizacional de TI refleja de manera apropiada las necesidades del negocio proporcionando servicios alineados con los procesos estratégicos del negocio, en lugar de estar alineados con tecnologías aisladas.		**X**	
5 Optimizado cuando La estructura organizacional de TI es flexible y adaptable. Se ponen en funcionamiento las mejores prácticas de la industria. Existe un uso amplio de la tecnología para monitorear el desempeño de la organización y de los procesos de TI. La tecnología se aprovecha para apoyar la complejidad y distribución geográfica de la organización. Un proceso de mejora continua existe y está implantado.		**X**	

Tabla 13: MODELOS DE MADUREZ PO4

Fuente: Realizado por el autor

DOMINIO: PLANEAR Y ORGANIZAR PO5: Administrar la inversión en TI			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de Administrar la inversión de TI se encuentra en el nivel 1
0 No existente cuando No existe conciencia de la importancia de la selección y presupuesto de las inversiones en TI. No existe seguimiento o monitoreo de las inversiones y gastos de TI	**X**		
1 Inicial/Ad Hoc cuando La organización reconoce la necesidad de administrar la inversión en TI, aunque esta necesidad se comunica de manera inconsistente. La asignación de responsabilidades de selección de inversiones en TI y de desarrollo de presupuestos se hace de una forma ad hoc. Existen implantaciones aisladas de selección y presupuesto de inversiones en TI, con documentación informal. Las inversiones en TI se justifican de una forma ad hoc. Se toman decisiones presupuestales enfocadas de modo reactivo y operativo.		**X**	
2 Repetible pero intuitiva cuando Existe un entendimiento implícito de la necesidad de seleccionar y presupuestar las inversiones en TI. La necesidad de un proceso de selección y presupuesto se comunica. El cumplimiento depende de la iniciativa de individuos dentro de la organización. Surgen técnicas comunes para desarrollar componentes del presupuesto de TI. Se toman decisiones presupuestales reactivas y tácticas.		**X**	
3 Proceso definido cuando Las políticas y los procesos para inversiones y presupuestos están definidas, documentadas y comunicadas y cubren temas clave de negocio y de tecnología. El presupuesto de TI está alineado con los planes estratégicos de TI y con los planes del negocio. Los procesos de selección de inversiones en TI y de presupuestos están formalizados, documentados y comunicados. Surge el entrenamiento formal aunque todavía se basa de modo principal en iniciativas individuales. Ocurre la aprobación formal de la selección de inversiones en TI y presupuestos. El personal de TI cuenta con la experiencia y habilidades necesarias para desarrollar el presupuesto de TI y recomendar inversiones apropiadas en TI.		**X**	
4 Administrado y medible cuando La responsabilidad y la rendición de cuentas por la selección y presupuestos de inversiones se asignan a un individuo específico. Las diferencias en el presupuesto se identifican y se resuelven. Se realizan análisis formales de costos que cubren los costos directos e indirectos de las operaciones existentes, así como propuestas de inversiones, considerando todos los costos a lo largo del ciclo completo de vida. Se usa un proceso de presupuestos pro-activo y estándar. El impacto en los costos operativos y de desarrollo debidos a cambios de software, hasta cambios en integración de sistemas y recursos humanos de TI, se reconoce en los planes de inversión. Los beneficios y los retornos se calculan en términos financieros y no financieros.		**X**	
5 Optimizado cuando Se utilizan las mejores prácticas de la industria para evaluar los costos por comparación e identificar la efectividad de las inversiones. Se utiliza el análisis de los avances tecnológicos en el proceso de selección y presupuesto de inversiones. El proceso de administración de inversiones se mejora de forma continua con base en las lecciones aprendidas provenientes del análisis del desempeño real de las inversiones. Las decisiones de inversiones incluyen las tendencias de mejora de precio/desempeño. Se investigan y evalúan formalmente las alternativas de financiamiento dentro del contexto de la estructura de capital existente en la organización, mediante el uso de métodos formales de evaluación. Existe la identificación proactiva de varianzas. Se incluye un análisis de los costos y beneficios a largo plazo del ciclo de vida total en la toma de decisiones de inversión.		**X**	

Tabla 14: MODELOS DE MADUREZ PO5

DOMINIO: PLANEAR Y ORGANIZAR PO6: Comunicar las aspiraciones y la dirección de la gerencia			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de comunicar las aspiraciones y la dirección de la gerencia se encuentra en el nivel 3
0 No existente cuando La gerencia no ha establecido un ambiente positivo de control de información. No hay reconocimiento de la necesidad de establecer un conjunto de políticas, procedimientos, estándares y procesos de cumplimiento.	**X**		
1 Inicial/Ad Hoc cuando La gerencia es reactiva al resolver los requerimientos del ambiente de control de información. Las políticas, procedimientos estándares se elaboran y comunican de forma ad hoc de acuerdo a los temas. Los procesos de elaboración, comunicación y cumplimiento son informales e inconsistentes.	**X**		
2 Repetible pero intuitiva cuando La gerencia tiene un entendimiento implícito de las necesidades y de los requerimientos de un ambiente de control de información efectivo, aunque las prácticas son en su mayoría informales. La gerencia ha comunicado la necesidad de políticas, procedimientos y estándares de control, pero la elaboración se delega a la discreción de gerentes y áreas de negocio individuales. La calidad se reconoce como una filosofía deseable a seguir, pero las prácticas se dejan a discreción de gerentes individuales. El entrenamiento se realiza de forma individual, según se requiera.	**X**		
3 Proceso definido cuando La gerencia ha elaborado, documentado y comunicado un ambiente completo de administración de calidad y control de la información, que incluye un marco para las políticas, procedimientos y estándares. El proceso de elaboración de políticas es estructurado, mantenido y conocido por el personal, y las políticas, procedimientos y estándares existentes son razonablemente sólidos y cubren temas clave. La gerencia ha reconocido la importancia de la conciencia de la seguridad de TI y ha iniciado programas de concienciación. El entrenamiento formal está disponible para apoyar al ambiente de control de información, aunque no se aplica de forma rigurosa. Aunque existe un marco general de desarrollo para las políticas y estándares de control, el monitoreo del cumplimiento de estas políticas y estándares es inconsistente. Las técnicas para fomentar la conciencia de la seguridad están estandarizadas y formalizadas.		**X**	
4 Administrado y medible cuando La gerencia asume la responsabilidad de comunicar las políticas de control interno y delega la responsabilidad y asigna suficientes recursos para mantener el ambiente en línea con los cambios significativos. Se ha establecido un ambiente de control de información positivo y proactivo. Se ha establecido un juego completo de políticas, procedimientos y estándares, los cuales se mantienen y comunican, y forman un componente de buenas prácticas internas. Se ha establecido un marco de trabajo para la implantación y las verificaciones subsiguientes de cumplimiento.		**X**	
5 Optimizado cuando El ambiente de control de la información está alineado con el marco administrativo estratégico y con la visión, y con frecuencia se revisa, actualiza y mejora. Se asignan expertos internos y externos para garantizar que se adoptan las mejores prácticas de la industria, con respecto a las guías de control y a las técnicas de comunicación. El monitoreo, la auto-evaluación y las verificaciones de cumplimiento están extendidas en la organización. La tecnología se usa para mantener bases de conocimiento de políticas y de concienciación y para optimizar la comunicación, usando herramientas de automatización de oficina y de entrenamiento basado en computadora.		**X**	

Tabla 15: MODELOS DE MADUREZ PO6

Fuente: Realizado por el autor

DOMINIO: PLANEAR Y ORGANIZAR PO7: Administrar recursos humanos de TI			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de administrar recursos humanos de TI se encuentra en el nivel 3
0 No existente cuando No existe conciencia sobre la importancia de alinear la administración de recursos humanos de TI con el proceso de planeación de la tecnología para la organización. No hay persona o grupo formalmente responsable de la administración de los recursos humanos de TI.	**X**		
1 Inicial/Ad Hoc cuando La gerencia reconoce la necesidad de contar con administración de recursos humanos de TI. El proceso de administración de recursos humanos de TI es informal y reactivo. El proceso de recursos humanos de TI está enfocado de manera operacional en la contratación y administración del personal de TI. Se está desarrollando la conciencia con respecto al impacto que tienen los cambios rápidos de negocio y de tecnología, y las soluciones cada vez más complejas, sobre la necesidad de nuevos niveles de habilidades y de competencia.	**X**		
2 Repetible pero intuitiva cuando Existe un enfoque táctico para contratar y administrar al personal de TI, dirigido por necesidades específicas de proyectos, en lugar de hacerlo con base en un equilibrio entendido de disponibilidad interna y externa de personal calificado. Se imparte entrenamiento informal al personal nuevo, quienes después reciben entrenamiento según sea necesario.	**X**		
3 Proceso definido cuando Existe un proceso definido y documentado para administrar los recursos humanos de TI. Existe un plan de administración de recursos humanos. Existe un enfoque estratégico para la contratación y la administración del personal de TI. El plan de entrenamiento formal está diseñado para satisfacer las necesidades de los recursos humanos de TI. Está establecido un programa de rotación, diseñado para expandir las habilidades gerenciales y de negocio.		**X**	
4 Administrado y medible cuando La responsabilidad de la elaboración y el mantenimiento de un plan de administración de recursos humanos para TI ha sido asignada a un individuo o grupo con las habilidades y experiencia necesarias para elaborar y mantener el plan. El proceso para elaborar y mantener el plan de administración de recursos humanos de TI responde al cambio. La organización cuenta con métricas estandarizadas que le permiten identificar desviaciones respecto al plan de administración de recursos humanos de TI con énfasis especial en el manejo del crecimiento y rotación del personal. Las revisiones de compensación y de desempeño se están estableciendo y se comparan con otras organizaciones de TI y con las mejores prácticas de la industria. La administración de recursos humanos es proactiva, tomando en cuenta el desarrollo de un plan de carrera.		**X**	
5 Optimizado cuando El plan de administración de recursos humanos de TI se actualiza de forma constante para satisfacer los cambiantes requerimientos del negocio. La administración de recursos humanos de TI está integrada y responde a la dirección estratégica de la entidad. Los componentes de la administración de recursos humanos de TI son consistentes con las mejores prácticas de la industria, tales como compensación, revisiones de desempeño, participación en foros de la industria, transferencia de conocimiento, entrenamiento y adiestramiento. Los programas de entrenamiento se desarrollan para todos los nuevos estándares tecnológicos y productos antes de su implantación en la organización.		**X**	

Tabla 16: MODELOS DE MADUREZ PO7

Fuente: Realizado por el autor

DOMINIO: PLANEAR Y ORGANIZAR PO9: Evaluar y administrar riesgos de TI			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de evaluar y administrar riesgos de TI se encuentra en el nivel 2.
0 No existente cuando La evaluación de riesgos para los procesos y las decisiones de negocio no ocurre. La organización no toma en cuenta los impactos en el negocio asociados a las vulnerabilidades de seguridad y a las incertidumbres del desarrollo de proyectos. La administración de riesgos no se ha identificado como algo relevante para adquirir soluciones de TI y para prestar servicios de TI	**X**		
1 Inicial/Ad Hoc cuando Los riesgos de TI se toman en cuenta de manera ad hoc. Se realizan evaluaciones informales de riesgos según lo determine cada proyecto. En algunas ocasiones se identifican evaluaciones de riesgos en un plan de proyectos pero se asignan a gerentes específicos con poca frecuencia. Los riesgos específicos relacionados con TI tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto. Los riesgos relativos a TI que afectan las operaciones del día con día, son rara vez discutidas en reuniones gerenciales. Cuando se toman en cuenta los riesgos, la mitigación es inconsistente. Existe un entendimiento emergente de que los riesgos de TI son importantes y necesitan ser considerados.	**X**		
2 Repetible pero intuitiva cuando Existe un enfoque de evaluación de riesgos inmaduro y en evolución y se implanta a discreción de los gerentes de proyecto. La administración de riesgos se da por lo general a altos niveles y se aplica de manera típica solo a proyectos grandes o como respuesta a problemas. Los procesos de mitigación de riesgos están en implantación donde se identifican riesgos.		**X**	
3 Proceso definido cuando Una política de administración de riesgos para toda la organización define cuándo y cómo realizar las evaluaciones de riesgos. La administración de riesgos sigue un proceso definido el cual está documentado. El entrenamiento sobre administración de riesgos está disponible para todo el personal. La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento se delega a la discreción del individuo. La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgos claves sean identificados. Un proceso para mitigar los riesgos clave por lo general se institucionaliza una vez que los riesgos se identifican. Las descripciones de puestos toman en cuenta las responsabilidades de administración de riesgos.		**X**	
4 Administrado y medible cuando Una política de administración de riesgos para toda la organización define cuándo y cómo realizar las evaluaciones de riesgos. La administración de riesgos sigue un proceso definido el cual está documentado. El entrenamiento sobre administración de riesgos está disponible para todo el personal. La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento se delega a la discreción del individuo. La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgos claves sean identificados. Un proceso para mitigar los riesgos clave por lo general se institucionaliza una vez que los riesgos se identifican. Las descripciones de puestos toman en cuenta las responsabilidades de administración de riesgos.		**X**	
5 Optimizado cuando La administración de riesgos ha evolucionado al nivel en que un proceso estructurado está implantado en toda la organización y es bien administrado. Las buenas prácticas se aplican en toda la organización. La captura, análisis y reporte de los datos de administración de riesgos están altamente automatizados. La orientación se toma de los líderes en el campo y la organización de TI participa en grupos de interés para intercambiar experiencias. La administración de riesgos está altamente integrada en todo el negocio y en las operaciones de TI está bien aceptada, y abarca a los usuarios de servicios de TI. La dirección detectará y actuará cuando se realicen decisiones grandes de inversión, operación o de TI, sin tomar en cuenta el plan de administración de riesgos. La dirección evalúa las estrategias de mitigación de riesgos de manera continua.		**X**	

Tabla 17: MODELOS DE MADUREZ PO9

DOMINIO: PLANEAR Y ORGANIZAR PO10: Administrar proyectos			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de administrar proyectos se encuentra en el nivel 2.
0 No existente cuando Las técnicas de administración de proyectos no se usan y la organización no toma en cuenta los impactos al negocio asociados con la mala administración de los proyectos y con las fallas de desarrollo en el proyecto.	**X**		
1 Inicial/Ad Hoc cuando El uso de técnicas y enfoques de administración de proyectos dentro de TI es una decisión individual que se deja a los gerentes de TI. Existe una carencia de compromiso por parte de la gerencia hacia la propiedad de proyectos y hacia la administración de proyectos. Las decisiones críticas sobre administración de proyectos se realizan sin la intervención de la gerencia usuaria ni del cliente. Hay poca o nula participación del cliente y del usuario para definir los proyectos de TI. No hay una organización clara dentro de TI para la administración de proyectos. Los roles y responsabilidades para la administración de proyectos no están definidas. Los proyectos, calendarios y puntos clave están definidos pobremente, si es que lo están. No se hace seguimiento al tiempo y a los gastos del equipo del proyecto y no se comparan con el presupuesto.	**X**		
2 Repetible pero intuitiva cuando La alta dirección ha obtenido y comunicado la conciencia de la necesidad de una administración de los proyectos de TI. La organización está en proceso de desarrollar y utilizar algunas técnicas y métodos de proyecto a proyecto. Los proyectos de TI han definido objetivos técnicos y de negocio de manera informal. Hay participación limitada de los interesados en la administración de los proyectos de TI. Las directrices iniciales se han elaborado para muchos aspectos de la administración de proyectos. La aplicación a proyectos de las directrices administrativas se deja a discreción del gerente de proyecto.		**X**	
3 Proceso definido cuando El proceso y la metodología de administración de proyectos de TI han sido establecidos y comunicados. Los proyectos de TI se definen con los objetivos técnicos y de negocio adecuados. La alta dirección del negocio y de TI, empiezan a comprometerse y a participar en la administración de los proyectos de TI. Se ha establecido una oficina de administración de proyectos dentro de TI, con roles y responsabilidades iniciales definidas. Los proyectos de TI se monitorean, con puntos clave, calendarios y mediciones de presupuesto y desempeño definidos y actualizados. Existe entrenamiento para la administración de proyectos. El entrenamiento en administración de proyectos es un resultado principalmente de las iniciativas individuales del equipo. Los procedimientos de aseguramiento de calidad y las actividades de implantación post-sistema han sido definidos, pero no se aplican de manera amplia por parte de los gerentes de TI. Los proyectos se empiezan a administrar como portafolios.		**X**	
4 Administrado y medible cuando La gerencia requiere que se revisen métricas y lecciones aprendidas estandarizadas y formales después de terminar cada proyecto. La administración de proyectos se mide y evalúa a través de la organización y no solo en TI. Las mejoras al proceso de administración de proyectos se formalizan y comunican y los miembros del equipo reciben entrenamiento sobre estas mejoras. La gerencia de TI ha implantado una estructura organizacional de proyectos con roles, responsabilidades y criterios de desempeño documentados. Los criterios para evaluar el éxito en cada punto clave se han establecido. El valor y el riesgo se miden y se administran, antes, durante y al final de los proyectos. Cada vez más, los proyectos abordan las metas organizacionales, en lugar de abordar solamente las específicas a TI. Existe un apoyo fuerte y activo a los proyectos por parte de los patrocinadores de la alta dirección, así como de los interesados. El entrenamiento relevante sobre administración de proyectos se planea para el equipo en la oficina de proyectos y a lo largo de la función de TI.		**X**	

5 Optimizado cuando Se encuentra implantada una metodología comprobada de ciclo de vida de proyectos, la cual se refuerza y se integra en la cultura de la organización completa. Se ha implantado una iniciativa continua para identificar e institucionalizar las mejores prácticas de administración de proyectos. Se ha definido e implantado una estrategia de TI para contratar el desarrollo y los proyectos operativos. La oficina integrada de administración de proyectos es responsable de los proyectos y programas desde su concepción hasta su post-implantación. La planeación de programas y proyectos en toda la organización garantiza que los recursos de TI y del usuario se utilizan de la mejor manera para apoyar las iniciativas estratégicas.		**X**	

Tabla 18: MODELOS DE MADUREZ PO10

Fuente: Realizado por el autor

DOMINIO: ADQUIRIR E IMPLANTAR **AI1: Identificar soluciones automatizadas**			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de identificar soluciones automatizadas se encuentra en el nivel 3
0 No existente cuando La organización no requiere de la identificación de los requerimientos funcionales y operativos para el desarrollo, implantación o modificación de soluciones, tales como sistemas, servicios, infraestructura y datos. La organización no está consciente de las soluciones tecnológicas disponibles que son potencialmente relevantes para su negocio.	**X**		
1 Inicial/Ad Hoc cuando Existe conciencia de la necesidad de definir requerimientos y de identificar soluciones tecnológicas. Grupos individuales se reúnen para analizar las necesidades de manera informal y los requerimientos se documentan algunas veces. Los individuos identifican soluciones con base en una conciencia limitada de mercado o como respuesta a ofertas de proveedores. Existe una investigación o análisis estructurado mínimo de la tecnología disponible.	**X**		
2 Repetible pero intuitiva cuando Existen algunos enfoques intuitivos para identificar que existen soluciones de TI y éstos varían a lo largo del negocio. Las soluciones se identifican de manera informal con base en la experiencia interna y en el conocimiento de la función de TI. El éxito de cada proyecto depende de la experiencia de unos cuantos individuos clave. La calidad de la documentación y de la toma de decisiones varía de forma considerable. Se usan enfoques no estructurados para definir los requerimientos e identificar las soluciones tecnológicas.	**X**		
3 Proceso definido cuando Existen enfoques claros y estructurados para determinar las soluciones de TI. El enfoque para la determinación de las soluciones de TI requiere la consideración de alternativas evaluadas contra los requerimientos del negocio o del usuario, las oportunidades tecnológicas, la factibilidad económica, las evaluaciones de riesgo y otros factores. El proceso para determinar las soluciones de TI se aplica para algunos proyectos con base en factores tales como las decisiones tomadas por el personal involucrado, la cantidad de tiempo administrativo dedicado, y el tamaño y prioridad del requerimiento de negocio original. Se usan enfoques estructurados para definir requerimientos e identificar soluciones de TI.		**X**	
4 Administrado y medible cuando Existe una metodología establecida para la identificación y la evaluación de las soluciones de TI y se usa para la mayoría de los proyectos. La documentación de los proyectos es de buena calidad y cada etapa se aprueba adecuadamente. Los requerimientos están bien articulados y de acuerdo con las estructuras predefinidas. Se consideran soluciones alternativas, incluyendo el análisis de costos y beneficios. La metodología es clara, definida, generalmente entendida y medible. Existe una interfaz definida de forma clara entre la gerencia de TI y la del negocio para la identificación y evaluación de las soluciones de TI.		**X**	

5 Optimizado cuando La metodología para la identificación y evaluación de las soluciones de TI está sujeta a una mejora continua. La metodología de adquisición e implantación tiene la flexibilidad para proyectos de grande y de pequeña escala. La metodología está soportada en bases de datos de conocimiento internas y externas que contienen material de referencia sobre soluciones tecnológicas. La metodología en sí misma genera documentación en una estructura predefinida que hace que la producción y el mantenimiento sean eficientes. Con frecuencia, se identifican nuevas oportunidades de uso de la tecnología para ganar una ventaja competitiva, ejercer influencia en la re-ingeniería de los procesos de negocio y mejorar la eficiencia en general. La gerencia detecta y toma medidas si las soluciones de TI se aprueban sin considerar tecnologías alternativas o los requerimientos funcionales del negocio.		**X**	

Tabla 19: MODELOS DE MADUREZ AI1

Fuente: Realizado por el autor

DOMINIO: ADQUIRIR E IMPLANTAR **AI2: Adquirir y mantener el software aplicativo**			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de adquirir y mantener el software aplicativo se encuentra en el nivel 3
0 No existente cuando No existe un proceso de diseño y especificación de aplicaciones. Típicamente, las aplicaciones se obtienen con base en ofertas de proveedores, en el reconocimiento de la marca o en la familiaridad del personal de TI con productos específicos, considerando poco o nada los requerimientos actuales.	**X**		
1 Inicial/Ad Hoc cuando Existe conciencia de la necesidad de contar con un proceso de adquisición y mantenimiento de aplicaciones. Los enfoques para la adquisición y mantenimientos de software aplicativo varían de un proyecto a otro. Es probable que se hayan adquirido en forma independiente una variedad de soluciones individuales para requerimientos particulares del negocio, teniendo como resultado ineficiencias en el mantenimiento y soporte. Se tiene poca consideración hacia la seguridad y disponibilidad de la aplicación en el diseño o adquisición de software aplicativo.	**X**		
2 Repetible pero intuitiva cuando Existen procesos de adquisición y mantenimiento de aplicaciones, con diferencias pero similares, en base a la experiencia dentro de la operación de TI. El mantenimiento es a menudo problemático y se resiente cuando se pierde el conocimiento interno de la organización. Se tiene poca consideración hacia la seguridad y disponibilidad de la aplicación en el diseño o adquisición de software aplicativo.	**X**		
3 Proceso definido cuando Existe un proceso claro, definido y de comprensión general para la adquisición y mantenimiento de software aplicativo. Este proceso va de acuerdo con la estrategia de TI y del negocio. Se intenta aplicar los procesos de manera consistente a través de diferentes aplicaciones y proyectos. Las metodologías son por lo general, inflexibles y difíciles de aplicar en todos los casos, por lo que es muy probable que se salten pasos. Las actividades de mantenimiento se planean, programan y coordinan.		**X**	
4 Administrado y medible cuando Existe una metodología formal y bien comprendida que incluye un proceso de diseño y especificación, un criterio de adquisición, un proceso de prueba y requerimientos para la documentación. Existen mecanismos de aprobación documentados y acordados, para garantizar que se sigan todos los pasos y se autoricen las excepciones. Han evolucionado prácticas y procedimientos para ajustarlos a la medida de la organización, los utilizan todo el personal y son apropiados para la mayoría de los requerimientos de aplicación.		**X**	

5 Optimizado cuando Las prácticas de adquisición y mantenimiento de software aplicativo se alinean con el proceso definido. El enfoque es con base en componentes, con aplicaciones predefinidas y estandarizadas que corresponden a las necesidades del negocio. El enfoque se extiende para toda la empresa. La metodología de adquisición y mantenimiento presenta un buen avance y permite un posicionamiento estratégico rápido, que permite un alto grado de reacción y flexibilidad para responder a requerimientos cambiantes del negocio. La metodología de adquisición e implantación de software aplicativo ha sido sujeta a mejora continua y se soporta con bases de datos internas y externas que contienen materiales de referencia y las mejores prácticas. La metodología produce documentación dentro de una estructura predefinida que hace eficiente la producción y mantenimiento.		**X**	

Tabla 20: MODELOS DE MADUREZ AI2

Fuente: Realizado por el autor

DOMINIO: ADQUIRIR E IMPLANTAR **AI3: Adquirir y mantener la infraestructura tecnológica**			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de adquirir y mantener la infraestructura tecnológica se encuentra en el nivel 3.
0 No existente cuando No se reconoce la administración de la infraestructura de tecnología como un asunto importante al cual deba ser resuelto.	**X**		
1 Inicial/Ad Hoc cuando Se realizan cambios a la infraestructura para cada nueva aplicación, sin ningún plan en conjunto. Aunque se tiene la percepción de que la infraestructura de TI es importante, no existe un enfoque general consistente. La actividad de mantenimiento reacciona a necesidades de corto plazo. El ambiente de producción es el ambiente de prueba.	**X**		
2 Repetible pero intuitiva cuando No hay consistencia entre enfoques tácticos al adquirir y dar mantenimiento a la infraestructura de TI. La adquisición y mantenimiento de la infraestructura de TI no se basa en una estrategia definida y no considera las necesidades de las aplicaciones del negocio que se deben respaldar. Se tiene la noción de que la infraestructura de TI es importante, que se apoya en algunas prácticas formales. Algunos mantenimientos se programan, pero no se programa ni se coordina en su totalidad. Para algunos ambientes, existe un ambiente de prueba por separado.	**X**		
3 Proceso definido cuando Existe un claro, definido y generalmente entendido proceso para adquirir y dar mantenimiento a la infraestructura TI. El proceso respalda las necesidades de las aplicaciones críticas del negocio y concuerda con la estrategia de negocio de TI, pero no se aplica en forma consistente. Se planea, programa y coordina el mantenimiento. Existen ambientes separados para prueba y producción.		**X**	
4 Administrado y medible cuando Se desarrolla el proceso de adquisición y mantenimiento de la infraestructura de tecnología a tal punto que funciona bien para la mayoría de las situaciones, se le da un seguimiento consistente y un enfoque hacia la reutilización. La infraestructura de TI soporta adecuadamente las aplicaciones del negocio. El proceso está bien organizado y es preventivo. Tanto el costo como el tiempo de realización para alcanzar el nivel esperado de escalamiento, flexibilidad e integración se han optimizado parcialmente.		**X**	

5 Optimizado cuando El proceso de adquisición y mantenimiento de la infraestructura de tecnología es preventivo y está estrechamente en línea con las aplicaciones críticas del negocio y con la arquitectura de la tecnología. Se siguen buenas prácticas respecto a las soluciones de tecnología, y la organización tiene conciencia de las últimas plataformas desarrolladas y herramientas de administración. Se reducen costos al racionalizar y estandarizar los componentes de la infraestructura y con el uso de la automatización. Con un alto nivel de conciencia se pueden identificar los medios óptimos para mejorar el desempeño en forma preventiva, incluyendo el considerar la opción de contratar servicios externos. La infraestructura de TI se entiende como el apoyo clave para impulsar el uso de TI		**X**	

Tabla 21: MODELOS DE MADUREZ AI3

Fuente: Realizado por el autor

DOMINIO: ADQUIRIR E IMPLANTAR AI4: Facilitar la operación y el uso			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de facilitar la operación y el uso se encuentra en el nivel 3.
0 No existente cuando No existe el proceso con respecto a la producción de documentación de usuario, manuales de operación y material de entrenamiento. Los únicos materiales existentes son aquellos que se suministran con los productos que se adquieren.	**X**		
1 Inicial/Ad Hoc cuando Existe la percepción de que la documentación de proceso es necesaria. La documentación se genera ocasionalmente y se distribuye en forma desigual a grupos limitados. Mucha de la documentación y muchos de los procedimientos ya caducaron. Los materiales de entrenamiento tienden a ser esquemas únicos con calidad variable. Virtualmente no existen procedimientos de integración a través de los diferentes sistemas y unidades de negocio. No hay aportes de las unidades de negocio en el diseño de programas de entrenamiento.	**X**		
2 Repetible pero intuitiva cuando Se utilizan enfoques similares para generar procedimientos y documentación, pero no se basan en un enfoque estructural o marco de trabajo. No hay un enfoque uniforme para el desarrollo de procedimientos de usuario y de operación. Individuos o equipos de proyecto generan los materiales de entrenamiento, y la calidad depende de los individuos que se involucran. Los procedimientos y la calidad del soporte al usuario van desde pobre a muy buena, con una consistencia e integración muy pequeña a lo largo de la organización. Se proporcionan o facilitan programas de entrenamiento para el negocio y los usuarios, pero no hay un plan general para ofrecer o dar entrenamiento.	**X**		
3 Proceso definido cuando Existe un esquema bien definido, aceptado y comprendido para documentación del usuario, manuales de operación y materiales de entrenamiento. Se guardan y se mantienen los procedimientos en una biblioteca formal y cualquiera que necesite saber tiene acceso a ella. Las correcciones a la documentación y a los procedimientos se realizan por reacción. Los procedimientos se encuentran disponibles fuera de línea y se pueden acceder y mantener en caso de desastre. Existe un proceso que especifica las actualizaciones de procedimientos y los materiales de entrenamiento para que sea un entregable explícito de un proyecto de cambio. A pesar de la existencia de enfoques definidos, el contenido actual varía debido a que no hay un control para reforzar el cumplimiento de estándares. Los usuarios se involucran en los procesos informalmente. Cada vez se utilizan más herramientas automatizadas en la generación y distribución de procedimientos. Se planea y programa tanto el entrenamiento del negocio como de los usuario.		**X**	
4 Administrado y medible cuando Existe un esquema definido para los procedimientos de mantenimiento y para los materiales de entrenamiento que cuentan con el soporte de la administración de TI. El enfoque considerado para los procedimientos de mantenimiento y los manuales de entrenamiento cubren todos los sistemas y las unidades de negocio, de manera que se pueden observar los procesos desde una perspectiva de negocio. Los procedimientos y materiales de entrenamiento se integran para que contengan interdependencias e interfases. Existen controles para garantizar que se adhieren los estándares y que se desarrollan y mantienen procedimientos para todos los procesos. La retroalimentación del negocio y del usuario sobre la documentación y el entrenamiento se recopila y evalúa como		**X**	

parte de un proceso continuo de mejora. Los materiales de documentación y entrenamiento se encuentran generalmente a un buen nivel, predecible, de confiabilidad y disponibilidad. Se implanta un proceso emergente para el uso de documentación y administración automatizada de procedimiento. El desarrollo automatizado de procedimientos se integra cada vez más con el desarrollo de sistemas aplicativos, facilitando la consistencia y el acceso al usuario. El entrenamiento de negocio y usuario es sensible a las necesidades del negocio. La administración de TI está desarrollando medidas para el desarrollo y la entrega de documentación, materiales y programas de entrenamiento.			
5 Optimizado cuando El proceso para la documentación de usuario y de operación se mejora constantemente con la adopción de nuevas herramientas o métodos. Los materiales de procedimiento y de entrenamiento se tratan como una base de conocimiento en evolución constante que se mantiene en forma electrónica, con el uso de administración de conocimiento actualizada, workflow y tecnologías de distribución, que los hacen accesibles y fáciles de mantener. El material de documentación y entrenamiento se actualiza para reflejar los cambios en la organización, en la operación y en el software. Tanto el desarrollo de materiales de documentación y entrenamiento como la entrega de programas de entrenamiento, se encuentran completamente integrados con el negocio y con las definiciones de proceso del negocio, siendo así un apoyo a los requerimientos de toda la organización y no tan sólo procedimientos orientados a TI.		**X**	

Tabla 22: MODELOS DE MADUREZ AI4

Fuente: Realizado por el autor

DOMINIO: ADQUIRIR E IMPLANTAR AI5: Adquirir recursos de TI			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de Adquirir recursos de TI se encuentra en el nivel 1.
0 No existente cuando No existe un proceso definido de adquisición de recursos de TI. La organización no reconoce la necesidad de tener políticas y procedimientos claros de adquisición para garantizar que todos los recursos de TI se encuentren disponibles y de forma oportuna y rentable.	**X**		
1 Inicial/Ad Hoc cuando La organización ha reconocido la necesidad de tener políticas y procedimientos documentados que enlacen la adquisición de TI con el proceso general de adquisiciones de la organización. Los contratos para la adquisición de recursos de TI son elaborados y administrados por gerentes de proyecto y otras personas que ejercen su juicio profesional más que seguir resultados de procedimientos y políticas formales. Sólo existe un relación *ad hoc* entre los procesos de administración de adquisiciones y contratos corporativos y TI. Los contratos de adquisición se administran a la terminación de los proyectos más que sobre una base continua.		**X**	
2 Repetible pero intuitiva cuando Existe conciencia organizacional de la necesidad de tener políticas y procedimientos básicos para la adquisición de TI. Las políticas y procedimientos se integran parcialmente con el proceso general de adquisición de la organización del negocio. Los procesos de adquisición se utilizan principalmente en proyectos mayores y bastante visibles. Se determinan responsabilidades y rendición de cuentas para la administración de adquisición y contrato de TI según la experiencia particular del gerente de contrato. Se reconoce la importancia de administrar proveedores y las relaciones con ellos, pero se manejan con base en la iniciativa individual. Los procesos de contrato se utilizan principalmente en proyectos mayores o muy visibles.		**X**	

3 Proceso definido cuando La administración establece políticas y procedimientos para la adquisición de TI. Las políticas y procedimientos toman como guía el proceso general de adquisición de la organización. La adquisición de TI se integra en gran parte con los sistemas generales de adquisición del negocio. Existen estándares de TI para la adquisición de recursos de TI. Los proveedores de recursos de TI se integran dentro de los mecanismos de administración de proyectos de la organización desde una perspectiva de administración de contratos. La administración de TI comunica la necesidad de contar con una administración adecuada de adquisiciones y contratos en toda la función de TI.		**X**	
4 Administrado y medible cuando La adquisición de TI se integra totalmente con los sistemas generales de adquisición de la organización. Se utilizan los estándares para la adquisición de recursos de TI en todos los procesos de adquisición. Se toman medidas para la administración de contratos y adquisiciones relevantes para los casos de negocio que requieran la adquisición de TI. Se dispone de reportes que sustentan los objetivos de negocio. La administración está consciente por lo general, de las excepciones a las políticas y procedimientos para la adquisición de TI. Se está desarrollando una administración estratégica de relaciones. La administración de TI implanta el uso de procesos de administración para adquisición y contratos en todas las adquisiciones mediante la revisión de medición al desempeño.		**X**	
5 Optimizado cuando La administración instituye y da recursos a procesos exhaustivos para la adquisición de TI. La administración impulsa el cumplimiento de las políticas y procedimientos de adquisición de TI. Se toman las medidas en la administración de contratos y adquisiciones, relevantes en casos de negocio para adquisición de TI. Se establecen buenas relaciones con el tiempo con la mayoría de los proveedores y socios, y se mide y vigila la calidad de estas relaciones. Se manejan las relaciones en forma estratégica. Los estándares, políticas y procedimientos de TI para la adquisición de recursos TI se manejan estratégicamente y responden a la medición del proceso. La administración de TI comunica la importancia estratégica de tener una administración apropiada de adquisiciones y contratos, a través de la función TI.		**X**	

Tabla 23: MODELOS DE MADUREZ AI5

Fuente: Realizado por el autor

DOMINIO: ADQUIRIR E IMPLANTAR **AI6: Administrar cambios**			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de administrar cambios se encuentra en el nivel 1.
0 No existente cuando No existe un proceso definido de administración de cambio y los cambios se pueden realizar virtualmente sin control. No hay conciencia de que el cambio puede causar una interrupción para TI y las operaciones del negocio y no hay conciencia de los beneficios de la buena administración de cambio.	**X**		
1 Inicial/Ad Hoc cuando Se reconoce que los cambios se deben administrar y controlar. Las prácticas varían y es muy probable que se puedan dar cambios sin autorización. Hay documentación de cambio pobre o no existente y la documentación de configuración es incompleta y no confiable. Es posible que ocurran errores junto con interrupciones al ambiente de producción, provocados por una pobre administración de cambios.		**X**	
2 Repetible pero intuitiva cuando Existe un proceso de administración de cambio informal y la mayoría de los cambios siguen este enfoque; sin embargo, el proceso no está estructurado, es rudimentario y propenso a errores. La exactitud de la documentación de la configuración es inconsistente y de planeación limitada y la evaluación de impacto se da previa al cambio.		**X**	

3 Proceso definido cuando Existe un proceso formal definido para la administración del cambio, que incluye la categorización, asignación de prioridades, procedimientos de emergencia, autorización del cambio y administración de liberación, y va surgiendo el cumplimiento. Se dan soluciones temporales a los problemas y los procesos a menudo se omiten o se hacen a un lado. Aún pueden ocurrir errores y los cambios no autorizados ocurren ocasionalmente. El análisis de impacto de los cambios de TI en operaciones de negocio se está volviendo formal, para apoyar la implantación planeada de nuevas aplicaciones y tecnologías.		**X**	
4 Administrado y medible cuando El proceso de administración de cambio se desarrolla bien y es consistente para todos los cambios, y la gerencia confía que hay excepciones mínimas. El proceso es eficiente y efectivo, pero se basa en manuales de procedimientos y controles considerables para garantizar el logro de la calidad. Todos los cambios están sujetos a una planeación minuciosa y a la evaluación del impacto para minimizar la probabilidad de tener problemas de post-producción. Se da un proceso de aprobación para cambios. La documentación de administración de cambios es vigente y correcta, con seguimiento formal a los cambios. La documentación de configuración es generalmente exacta. La planeación e implantación de la administración de cambios en TI se van integrando con los cambios en los procesos de negocio, para asegurar que se resuelven los asuntos referentes al entrenamiento, cambio organizacional y continuidad del negocio. Existe una coordinación creciente entre la administración de cambio de TI y el rediseño del proceso de negocio. Hay un proceso consistente para monitorear la calidad y el desempeño del proceso de administración de cambios.		**X**	
5 Optimizado cuando El proceso de administración de cambios se revisa con regularidad y se actualiza para permanecer en línea con las buenas prácticas. El proceso de revisión refleja los resultados del monitoreo. La información de la configuración es computarizada y proporciona un control de versión. El rastreo del cambio es sofisticado e incluye herramientas para detectar software no autorizado y sin licencia. La administración de cambio de TI se integra con la administración de cambio del negocio para garantizar que TI sea un factor que hace posible el incremento de productividad y la creación de nuevas oportunidades de negocio para la organización.		**X**	

Tabla 24: MODELOS DE MADUREZ AI6

Fuente: Realizado por el autor

DOMINIO: ADQUIRIR E IMPLANTAR **AI7: Instalar y acreditar soluciones y cambios**			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	
0 No existente cuando Hay una ausencia completa de procesos formales de instalación o acreditación y ni la gerencia señor, ni el personal de TI reconocen la necesidad de verificar que las soluciones se ajustan para el propósito deseado.	**X**		**GRADO DE MADUREZ.** El proceso de instalar y acreditar soluciones y cambios se encuentra en el nivel 3.
1 Inicial/Ad Hoc cuando Existe la percepción de la necesidad de verificar y confirmar que las soluciones implantadas sirven para el propósito esperado. Las pruebas se realizan para algunos proyectos, pero la iniciativa de pruebas se deja a los equipos de proyectos particulares y los enfoques que se toman varían. La acreditación formal y la autorización son raras o no existentes.	**X**		
2 Repetible pero intuitiva cuando Existe cierta consistencia entre los enfoques de prueba y acreditación, pero por lo regular no se basan en ninguna metodología. Los equipos individuales de desarrollo deciden normalmente el enfoque de prueba y casi siempre hay ausencia de pruebas de integración. Hay un proceso de aprobación informal.	**X**		

3 Proceso definido cuando Se cuenta con una metodología formal en relación con la instalación, migración, conversión y aceptación. Los procesos de TI para instalación y acreditación están integrados dentro del ciclo de vida del sistema y están automatizados hasta cierto punto. El entrenamiento, pruebas y transición y acreditación a producción tienen muy probablemente variaciones respecto al proceso definido, con base en las decisiones individuales. La calidad de los sistemas que pasan a producción es inconsistente, y los nuevos sistemas a menudo generan un nivel significativo de problemas posteriores a la implantación.		**X**	
4 Administrado y medible cuando Los procedimientos son formales y se desarrollan para ser organizados y prácticos con ambientes de prueba definidos y con procedimientos de acreditación. En la práctica, todos los cambios mayores de sistemas siguen este enfoque formal. La evaluación de la satisfacción a los requerimientos del usuario es estándar y medible, y produce mediciones que la gerencia puede revisar y analizar de forma efectiva. La calidad de los sistemas que entran en producción es satisfactoria para la gerencia, aún con niveles razonables de problemas posteriores a la implantación. La automatización del proceso es *ad hoc* y depende del proyecto. Es posible que la gerencia esté satisfecha con el nivel actual de eficiencia a pesar de la ausencia de una evaluación posterior a la implantación. El sistema de prueba refleja adecuadamente el ambiente de producción. La prueba de stress para los nuevos sistemas y la prueba de regresión para sistemas existentes se aplican para proyectos mayores.		**X**	
5 Optimizado cuando Los procesos de instalación y acreditación se han refinado a un nivel de buena práctica, con base en los resultados de mejora continua y refinamiento. Los procesos de TI para la instalación y acreditación están totalmente integrados dentro del ciclo de vida del sistema y se automatizan cuando es apropiado, arrojando el estatus más eficiente de entrenamiento, pruebas y transición a producción para los nuevos sistemas. Los ambientes de prueba bien desarrollados, los registros de problemas y los procesos de resolución de fallas aseguran la transición eficiente y efectiva al ambiente de producción. La acreditación toma lugar regularmente sin repetición de trabajos, y los problemas posteriores a la implantación se limitan normalmente a correcciones menores. Las revisiones posteriores a la implantación son estándar, y las lecciones aprendidas se canalizan nuevamente hacia el proceso para asegurar el mejoramiento continuo de la calidad. Las pruebas de stress para los nuevos sistemas y las pruebas de regresión para sistemas modificados se aplican en forma consistente.		**X**	

Tabla 25: MODELOS DE MADUREZ AI7

Fuente: Realizado por el autor

DOMINIO: ENTREGAR Y DAR SOPORTE **DS2: Administrar los servicios de terceros**			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	
0 No existente cuando Las responsabilidades y la rendición de cuentas no están definidas. No hay políticas y procedimientos formales respecto a la contratación con terceros. Los servicios de terceros no son ni aprobados ni revisados por la gerencia. No hay actividades de medición y los terceros no reportan. A falta de una obligación contractual de reportar, la alta gerencia no está al tanto de la calidad del servicio prestado.	**X**		**GRADO DE MADUREZ.** El proceso de Administrar los servicios de terceros se encuentra en el nivel 3.
1 Inicial/Ad Hoc cuando La gerencia está consciente de la importancia de la necesidad de tener políticas y procedimientos documentados para la administración de los servicios de terceros, incluyendo la firma de contratos. No hay condiciones estandarizadas para los convenios con los prestadores de servicios. La medición de los servicios prestados es informal y reactiva. Las prácticas dependen de la experiencia de los individuos y del proveedor (por ejemplo, por demanda).	**X**		

2 Repetible pero intuitiva cuando El proceso de supervisión de los proveedores de servicios de terceros, de los riesgos asociados y de la prestación de servicios es informal. Se utiliza un contrato pro-forma con términos y condiciones estándares del proveedor (por ejemplo, la descripción de servicios que se prestarán). Los reportes sobre los servicios existen, pero no apoyan los objetivos del negocio.	**X**		
3 Proceso definido cuando Hay procedimientos bien documentados para controlar los servicios de terceros con procesos claros para tratar y negociar con los proveedores. Cuando se hace un acuerdo de prestación de servicios, la relación con el tercero es meramente contractual. La naturaleza de los servicios a prestar se detalla en el contrato e incluye requerimientos legales, operacionales y de control. Se asigna la responsabilidad de supervisar los servicios de terceros. Los términos contractuales se basan en formatos estandarizados. El riesgo del negocio asociado con los servicios del tercero esta valorado y esta reportado.		**X**	
4 Administrado y medible cuando Se establecen criterios formales y estandarizados para definir los términos de un acuerdo, incluyendo alcance del trabajo, servicios/entregables a suministrar, suposiciones, calendario, costos, acuerdos de facturación y responsabilidades. Se asignan las responsabilidades para la administración del contrato y del proveedor. Las aptitudes, capacidades y riesgos del proveedor son verificadas de forma continua. Los requerimientos del servicio están definidos y alineados con los objetivos del negocio. Existe un proceso para comparar el desempeño contra los términos contractuales, lo cual proporciona información para evaluar los servicios actuales y futuros del tercero. Se utilizan modelos de fijación de precios de transferencia en el proceso de adquisición. Todas las partes involucradas tienen conocimiento de las expectativas del servicio, de los costos y de las etapas. Se acordaron los KPIs y KGIs para la supervisión del servicio.		**X**	
5 Optimizado cuando Los contratos firmados con los terceros son revisados de forma periódica en intervalos predefinidos. La responsabilidad de administrar a los proveedores y la calidad de los servicios prestados está asignada. Se monitorea el cumplimiento de las condiciones operacionales, legales y de control y se implantan acciones correctivas. El tercero está sujeto a revisiones periódicas independientes y se le retroalimenta sobre su desempeño para mejorar la prestación del servicio. Las mediciones varían como respuesta a los cambios en las condiciones del negocio. Las mediciones ayudan a la detección temprana de problemas potenciales con los servicios de terceros. La notificación completa y bien definida del cumplimiento de los niveles de servicio, está asociada con la compensación del tercero. La gerencia ajusta el proceso de adquisición y monitoreo de servicios de terceros con base en los resultados de los KPIs y KGIs.		**X**	

Tabla 26: MODELOS DE MADUREZ DS2

Fuente: Realizado por el autor

DOMINIO: ENTREGAR Y DAR SOPORTE **DS3: Administrar el desempeño y la capacidad**			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.**
0 No existente cuando La gerencia no reconoce que los procesos clave del negocio pueden requerir altos niveles de desempeño de TI o que el total de los requerimientos de servicios de TI del negocio pueden exceder la capacidad. No se lleva cabo un proceso de planeación de la capacidad.	**X**		El proceso de administrar el desempeño y la capacidad se encuentra en el

1 Inicial/Ad Hoc cuando Los usuarios, con frecuencia, tienen que llevar acabo soluciones alternas para resolver las limitaciones de desempeño y capacidad. Los responsables de los procesos del negocio valoran poco la necesidad de llevar a cabo una planeación de la capacidad y del desempeño. Las acciones para administrar el desempeño y la capacidad son típicamente reactivas. El proceso de planeación de la capacidad y el desempeño es informal. El entendimiento sobre la capacidad y el desempeño de TI, actual y futuro, es limitado.	**X**		nivel 2.
2 Repetible pero intuitiva cuando Los responsables del negocio y la gerencia de TI están conscientes del impacto de no administrar el desempeño y la capacidad. Las necesidades de desempeño se logran por lo general con base en evaluaciones de sistemas individuales y el conocimiento y soporte de equipos de proyecto. Algunas herramientas individuales pueden utilizarse para diagnosticar problemas de desempeño y de capacidad, pero la consistencia de los resultados depende de la experiencia de individuos clave. No hay una evaluación general de la capacidad de desempeño de TI o consideración sobre situaciones de carga pico y peor-escenario. Los problemas de disponibilidad son susceptibles de ocurrir de manera inesperada y aleatoria y toma mucho tiempo diagnosticarlos y corregirlos. Cualquier medición de desempeño se basa primordialmente en las necesidades de TI y no en las necesidades del cliente.		**X**	
3 Proceso definido cuando Los requerimientos de desempeño y capacidad están definidos a lo largo del ciclo de vida del sistema. Hay métricas y requerimientos de niveles de servicio bien definidos, que pueden utilizarse para medir el desempeño operacional. Los pronósticos de la capacidad y el desempeño se modelan por medio de un proceso definido. Los reportes se generan con estadísticas de desempeño. Los problemas relacionados al desempeño y a la capacidad siguen siendo susceptibles a ocurrir y su resolución sigue consumiendo tiempo. A pesar de los niveles de servicio publicados, los usuarios y los clientes pueden sentirse escépticos acerca de la capacidad del servicio.		**X**	
4 Administrado y medible cuando Los requerimientos de desempeño y capacidad están definidos a lo largo del ciclo de vida del sistema. Hay métricas y requerimientos de niveles de servicio bien definidos, que pueden utilizarse para medir el desempeño operacional. Los pronósticos de la capacidad y el desempeño se modelan por medio de un proceso definido. Los reportes se generan con estadísticas de desempeño. Los problemas relacionados al desempeño y a la capacidad siguen siendo susceptibles a ocurrir y su resolución sigue consumiendo tiempo. A pesar de los niveles de servicio publicados, los usuarios y los clientes pueden sentirse escépticos acerca de la capacidad del servicio.		**X**	
5 Optimizado cuando Los planes de desempeño y capacidad están completamente sincronizados con las proyecciones de demanda del negocio. La infraestructura de TI y la demanda del negocio están sujetas a revisiones regulares para asegurar que se logre una capacidad óptima con el menor costo posible. Las herramientas para monitorear recursos críticos de TI han sido estandarizadas y usadas a través de diferentes plataformas y vinculadas a un sistema de administración de incidentes a lo largo de toda la organización. Las herramientas de monitoreo detectan y pueden corregir automáticamente problemas relacionados con la capacidad y el desempeño. Se llevan a cabo análisis de tendencias, los cuales muestran problemas de desempeño inminentes causados por incrementos en los volúmenes de negocio, lo que permite planear y evitar problemas inesperados. Las métricas para medir el desempeño y la capacidad de TI han sido bien afinadas dentro de los KGIs y KPIs para todos los procesos de negocio críticos y se miden de forma regular. La gerencia ajusta la planeación del desempeño y la capacidad siguiendo los análisis de los KGIs y KPIs.		**X**	

Tabla 27: MODELOS DE MADUREZ DS3

Fuente: Realizado por el autor

DOMINIO: ENTREGAR Y DAR SOPORTE DS4: Garantizar la continuidad del servicio			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	
0 No existente cuando No hay entendimiento de los riesgos, vulnerabilidades y amenazas a las operaciones de TI o del impacto en el negocio por la pérdida de los servicios de TI. No se considera que la continuidad en los servicios deba tener atención de la gerencia.	**X**		**GRADO DE MADUREZ.** El proceso de garantizar la continuidad del servicio se encuentra en el nivel 2.
1 Inicial/Ad Hoc cuando Las responsabilidades sobre la continuidad de los servicios son informales y la autoridad para ejecutar responsabilidades es limitada. La gerencia comienza a darse cuenta de los riesgos relacionados y de la necesidad de mantener continuidad en los servicios. El enfoque de la gerencia sobre la continuidad del servicio radica en los recursos de infraestructura, en vez de radicar en los servicios de TI. Los usuarios utilizan soluciones alternas como respuesta a la interrupción de los servicios. La respuesta de TI a las interrupciones mayores es reactiva y sin preparación. Las pérdidas de energía planeadas están programadas para cumplir con las necesidades de TI pero no consideran los requerimientos del negocio.	**X**		
2 Repetible pero intuitiva cuando Se asigna la responsabilidad para mantener la continuidad del servicio. Los enfoques para asegurar la continuidad están fragmentados. Los reportes sobre la disponibilidad son esporádicos, pueden estar incompletos y no toman en cuenta el impacto en el negocio. No hay un plan de continuidad de TI documentado, aunque hay compromiso para mantener disponible la continuidad del servicio y sus principios más importantes se conocen. Existe un inventario de sistemas y componentes críticos, pero puede no ser confiable. Las prácticas de continuidad en los servicios emergen, pero el éxito depende de los individuos.		**X**	
3 Proceso definido cuando La responsabilidad sobre la administración de la continuidad del servicio es clara. Las responsabilidades de la planeación y de las pruebas de la continuidad de los servicios están claramente asignadas y definidas. El plan de continuidad de TI está documentado y basado en la criticidad de los sistemas y el impacto al negocio. Hay reportes periódicos de las pruebas de continuidad. Los individuos toman la iniciativa para seguir estándares y recibir capacitación para enfrentarse con incidentes mayores o desastres. La gerencia comunica de forma regular la necesidad de planear el aseguramiento de la continuidad del servicio. Se han aplicado componentes de alta disponibilidad y redundancia. Se mantiene un inventario de sistemas y componentes críticos.		**X**	
4 Administrado y medible cuando La responsabilidad sobre la administración de la continuidad del servicio es clara. Las responsabilidades de la planeación y de las pruebas de la continuidad de los servicios están claramente asignadas y definidas. El plan de continuidad de TI está documentado y basado en la criticidad de los sistemas y el impacto al negocio. Hay reportes periódicos de las pruebas de continuidad. Los individuos toman la iniciativa para seguir estándares y recibir capacitación para enfrentarse con incidentes mayores o desastres. La gerencia comunica de forma regular la necesidad de planear el aseguramiento de la continuidad del servicio. Se han aplicado componentes de alta disponibilidad y redundancia. Se mantiene un inventario de sistemas y componentes críticos.		**X**	

5 Optimizado cuando Se hacen cumplir las responsabilidades y los estándares para la continuidad de los servicios. Se asigna la responsabilidad de mantener un plan de continuidad de servicios. Las actividades de mantenimiento están basadas en los resultados de las pruebas de continuidad, en las buenas prácticas internas y en los cambios en el ambiente del negocio y de TI. Se recopila, analiza y reporta documentación estructurada sobre la continuidad en los servicios y se actúa en consecuencia. Se brinda capacitación formal y obligatoria sobre los procesos de continuidad. Se implementan regularmente buenas prácticas de disponibilidad de los sistemas. Las prácticas de disponibilidad y la planeación de la continuidad de los servicios tienen influencia una sobre la otra. Se clasifican los incidentes de discontinuidad y la ruta de escalamiento es bien conocida por todos los involucrados. Se han desarrollado y acordado KGIs y KPIs para la continuidad de los servicios, aunque pueden ser medidos de manera inconsistente.		**X**	

Tabla 28: MODELOS DE MADUREZ DS4

Fuente: Realizado por el autor

DOMINIO: ENTREGAR Y DAR SOPORTE **DS5: Garantizar la seguridad de los sistemas**			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de garantizar la seguridad de los sistemas se encuentra en el nivel 2.
0 No existente cuando La organización no reconoce la necesidad de la seguridad para TI. Las responsabilidades y la rendición de cuentas no están asignadas para garantizar la seguridad. Las medidas para soportar la administrar la seguridad de TI no están implementadas. No hay reportes de seguridad de TI ni un proceso de respuesta para resolver brechas de seguridad de TI. Hay una total falta de procesos reconocibles de administración de seguridad de sistemas.	**X**		
1 Inicial/Ad Hoc cuando La organización reconoce la necesidad de seguridad para TI. La conciencia de la necesidad de seguridad depende principalmente del individuo. La seguridad de TI se lleva a cabo de forma reactiva. No se mide la seguridad de TI. Las brechas de seguridad de TI ocasionan respuestas con acusaciones personales, debido a que las responsabilidades no son claras. Las respuestas a las brechas de seguridad de TI son impredecibles.	**X**		
2 Repetible pero intuitiva cuando Las responsabilidades y la rendición de cuentas sobre la seguridad, están asignadas a un coordinador de seguridad de TI, pero la autoridad gerencial del coordinador es limitada. La conciencia sobre la necesidad de la seguridad esta fraccionada y limitada. Aunque los sistemas producen información relevante respecto a la seguridad, ésta no se analiza. Los servicios de terceros pueden no cumplir con los requerimientos específicos de seguridad de la empresa. Las políticas de seguridad se han estado desarrollando, pero las herramientas y las habilidades son inadecuadas. Los reportes de la seguridad de TI son incompletos, engañosos o no aplicables. La capacitación sobre seguridad está disponible pero depende principalmente de la iniciativa del individuo. La seguridad de TI es vista primordialmente como responsabilidad y disciplina de TI, y el negocio no ve la seguridad de TI como parte de su propia disciplina.		**X**	
3 Proceso definido cuando Existe conciencia sobre la seguridad y ésta es promovida por la gerencia. Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI. Las responsabilidades de la seguridad de TI están asignadas y entendidas, pero no continuamente implementadas. Existe un plan de seguridad de TI y existen soluciones de seguridad motivadas por un análisis de riesgo. Los reportes no contienen un enfoque claro de negocio. Se realizan pruebas de seguridad adecuadas (por ejemplo, pruebas contra intrusos). Existe capacitación en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal.		**X**	

4 Administrado y medible cuando Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. Regularmente se lleva a cabo un análisis de impacto y de riesgos de seguridad. Las políticas y prácticas de seguridad se complementan con referencias de seguridad específicas. El contacto con métodos para promover la conciencia de la seguridad es obligatorio. La identificación, autenticación y autorización de los usuarios está estandarizada. La certificación en seguridad es buscada por parte del personal que es responsable de la auditoría y la administración de la seguridad. Las pruebas de seguridad se hacen utilizando procesos estándares y formales que llevan a mejorar los niveles de seguridad. Los procesos de seguridad de TI están coordinados con la función de seguridad de toda la organización. Los reportes de seguridad están ligados con los objetivos del negocio. La capacitación sobre seguridad se imparte tanto para TI como para el negocio. La capacitación sobre seguridad de TI se planea y se administra de manera que responda a las necesidades del negocio y a los perfiles de riesgo de seguridad. Los KGIs y KPIs ya están definidos pero no se miden aún.		**X**	
5 Optimizado cuando Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. Regularmente se lleva a cabo un análisis de impacto y de riesgos de seguridad. Las políticas y prácticas de seguridad se complementan con referencias de seguridad específicas. El contacto con métodos para promover la conciencia de la seguridad es obligatorio. La identificación, autenticación y autorización de los usuarios está estandarizada. La certificación en seguridad es buscada por parte del personal que es responsable de la auditoría y la administración de la seguridad. Las pruebas de seguridad se hacen utilizando procesos estándares y formales que llevan a mejorar los niveles de seguridad. Los procesos de seguridad de TI están coordinados con la función de seguridad de toda la organización. Los reportes de seguridad están ligados con los objetivos del negocio. La capacitación sobre seguridad se imparte tanto para TI como para el negocio. La capacitación sobre seguridad de TI se planea y se administra de manera que responda a las necesidades del negocio y a los perfiles de riesgo de seguridad. Los KGIs y KPIs ya están definidos pero no se miden aún.		**X**	

Tabla 29: MODELOS DE MADUREZ DS5

Fuente: Realizado por el autor

DOMINIO: ENTREGAR Y DAR SOPORTE DS7: Educar y entrenar a los usuarios			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de educar y entrenar a los usuarios se encuentra en el nivel 2.
0 No existente cuando Hay una total falta de programas de entrenamiento y educación. La organización no reconoce que hay un problema a ser atendido respecto al entrenamiento y no hay comunicación sobre el problema.	**X**		
1 Inicial/Ad Hoc cuando Hay evidencia de que la organización ha reconocido la necesidad de contar con un programa de entrenamiento y educación, pero no hay procedimientos estandarizados. A falta de un proceso organizado, los empleados han buscado y asistido a cursos de entrenamiento por su cuenta. Algunos de estos cursos de entrenamiento abordan los temas de conducta ética, conciencia sobre la seguridad en los sistemas y prácticas de seguridad. El enfoque global de la gerencia carece de cohesión y sólo hay comunicación esporádica e inconsistente respecto a los problemas y enfoques para hacerse cargo del entrenamiento y la educación.	**X**		
2 Repetible pero intuitiva cuando Hay conciencia sobre la necesidad de un programa de entrenamiento y educación, y sobre los procesos asociados a lo largo de toda la organización. El entrenamiento está comenzando a identificarse en los planes de desempeño individuales de los empleados. Los procesos se han desarrollado hasta la fase en la cual se imparte entrenamiento informal por parte de diferentes instructores, cubriendo los mismos temas de materias con diferentes puntos de vista. Algunas de las clases abordan los temas de conducta ética y de conciencia sobre prácticas y actividades de seguridad en los sistemas. Hay una gran dependencia del conocimiento de los individuos. Sin embargo, hay comunicación consistente sobre los problemas globales y sobre la necesidad de atenderlos.		**X**	

3 Proceso definido cuando El programa de entrenamiento y educación se institucionaliza y comunica, y los empleados y gerentes identifican y documentan las necesidades de entrenamiento. Los procesos de entrenamiento y educación se estandarizan y documentan. Para soportar el programa de entrenamiento y educación, se establecen presupuestos, recursos, instructores e instalaciones. Se imparten clases formales sobre conducta ética y sobre conciencia y prácticas de seguridad en los sistemas. La mayoría de los procesos de entrenamiento y educación son monitoreados, pero no todas las desviaciones son susceptibles de detección por parte de la gerencia. El análisis sobre problemas de entrenamiento y educación solo se aplica de forma ocasional.		**X**	
4 Administrado y medible cuando El programa de entrenamiento y educación se institucionaliza y comunica, y los empleados y gerentes identifican y documentan las necesidades de entrenamiento. Los procesos de entrenamiento y educación se estandarizan y documentan. Para soportar el programa de entrenamiento y educación, se establecen presupuestos, recursos, instructores e instalaciones. Se imparten clases formales sobre conducta ética y sobre conciencia y prácticas de seguridad en los sistemas. La mayoría de los procesos de entrenamiento y educación son monitoreados, pero no todas las desviaciones son susceptibles de detección por parte de la gerencia. El análisis sobre problemas de entrenamiento y educación solo se aplica de forma ocasional.		**X**	
5 Optimizado cuando Hay un programa completo de entrenamiento y educación que produce resultados medibles. Las responsabilidades son claras y se establece la propiedad sobre los procesos. El entrenamiento y la educación son componentes de los planes de carrera de los empleados. La gerencia apoya y asiste a sesiones de entrenamiento y de educación. Todos los empleados reciben entrenamiento sobre conducta ética y sobre conciencia y prácticas de seguridad en los sistemas. Todos los empleados reciben el nivel apropiado de entrenamiento sobre prácticas de seguridad en los sistemas para proteger contra daños originados por fallas que afecten la disponibilidad, la confidencialidad y la integridad. La gerencia monitorea el cumplimiento por medio de revisión constante y actualización del programa y de los procesos de entrenamiento. Los procesos están en vía de mejora y fomentan las mejores prácticas internas.		**X**	

Tabla 30: MODELOS DE MADUREZ DS7

Fuente: Realizado por el autor

DOMINIO: ENTREGAR Y DAR SOPORTE **DS8: Administrar la mesa de servicio y los incidentes**			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de administrar la mesa de servicio y los incidentes se encuentra en el nivel 2.
0 No existente cuando No hay soporte para resolver problemas y preguntas de los usuarios. Hay una completa falta de procesos para la administración de incidentes. La organización no reconoce que hay un problema que atender.	**X**		
1 Inicial/Ad Hoc cuando La gerencia reconoce que requiere un proceso soportado por herramientas y personal para responder a las consultas de los usuarios y administrar la resolución de incidentes. Sin embargo, se trata de un proceso no estandarizado y sólo se brinda soporte reactivo. La gerencia no monitorea las consultas de los usuarios, los incidentes o las tendencias. No existe un proceso de escalamiento para garantizar que los problemas se resuelvan.	**X**		
2 Repetible pero intuitiva cuando Hay conciencia organizacional de la necesidad de una función de mesa de servicio y de un proceso de administración de incidentes. Existe ayuda disponible de manera informal a través de una red de individuos expertos. Estos individuos tienen a su disposición algunas herramientas comunes para ayudar en la resolución de incidentes. No hay entrenamiento formal y la comunicación obre procedimientos estándar y la responsabilidad es delegada al individuo.		**X**	

3 Proceso definido cuando Hay conciencia organizacional de la necesidad de una función de mesa de servicio y de un proceso de administración de incidentes. Existe ayuda disponible de manera informal a través de una red de individuos expertos. Estos individuos tienen a su disposición algunas herramientas comunes para ayudar en la resolución de incidentes. No hay entrenamiento formal y la comunicación obre procedimientos estándar y la responsabilidad es delegada al individuo.		**X**	
4 Administrado y medible cuando En todos los niveles de la organización hay un total entendimiento de los beneficios de un proceso de administración de incidentes y la función de mesa de servicio se ha establecido en las unidades organizacionales apropiadas. Las herramientas y técnicas están automatizadas con una base de conocimientos centralizada. El personal de la mesa de servicio interactúa muy de cerca con el personal de administración de problemas. Las responsabilidades son claras y se monitorea su efectividad. Los procedimientos para comunicar, escalar y resolver incidentes han sido establecidos y comunicados. El personal de la mesa de servicio está capacitado y los procesos se mejoran a través del uso de software para tareas específicas. La gerencia ha desarrollado los KPIs y KGIs para el desempeño de la mesa de servicio.		**X**	
5 Optimizado cuando En todos los niveles de la organización hay un total entendimiento de los beneficios de un proceso de administración de incidentes y la función de mesa de servicio se ha establecido en las unidades organizacionales apropiadas. Las herramientas y técnicas están automatizadas con una base de conocimientos centralizada. El personal de la mesa de servicio interactúa muy de cerca con el personal de administración de problemas. Las responsabilidades son claras y se monitorea su efectividad. Los procedimientos para comunicar, escalar y resolver incidentes han sido establecidos y comunicados. El personal de la mesa de servicio está capacitado y los procesos se mejoran a través del uso de software para tareas específicas. La gerencia ha desarrollado los KPIs y KGIs para el desempeño de la mesa de servicio.		**X**	

Tabla 31: MODELOS DE MADUREZ DS8

Fuente: Realizado por el autor

DOMINIO: ENTREGAR Y DAR SOPORTE **DS9: Administrar la configuración**			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	
0 No existente cuando La gerencia no valora los beneficios de tener un proceso implementado que sea capaz de reportar y administrar las configuraciones de la infraestructura de TI, tanto para configuraciones de software.	**X**		**GRADO DE MADUREZ.** El proceso de administrar la configuración se encuentra en el nivel 2.
1 Inicial/Ad Hoc cuando Se reconoce la necesidad de contar con una administración de configuración. Se llevan a cabo tareas básicas de administración de configuraciones, tales como mantener inventarios de software pero de manera individual. No están definidas prácticas estandarizadas.	**X**		
2 Repetible pero intuitiva cuando La gerencia esta consciente de la necesidad de controlar la configuración de TI y entiende los beneficios de mantener información completa y precisa sobre las configuraciones, pero hay una dependencia implícita del conocimiento y experiencia del personal técnico. Las herramientas para la administración de configuraciones se utilizan hasta cierto grado, pero difieren entre plataformas. Además no se han definido prácticas estandarizadas de trabajo. El contenido de la información de la configuración es limitado y no lo utilizan los procesos interrelacionados, tales como administración de cambios y administración de problemas.		**X**	

3 Proceso definido cuando Los procedimientos y las prácticas de trabajo se han documentado, estandarizado y comunicado, pero la capacitación y la aplicación de estándares dependen del individuo. Además se han implementado herramientas similares de administración de configuración entre plataformas. Es poco probable detectar las desviaciones de los procedimientos y las verificaciones físicas se realizan de manera inconsistente. Se lleva a cabo algún tipo de automatización para ayudar a rastrear cambios en el software. La información de la configuración es utilizada por los procesos interrelacionados.		**X**	
4 Administrado y medible cuando En todos los niveles de la organización se reconoce la necesidad de administrar la configuración y las buenas prácticas siguen evolucionando. Los procedimientos y los estándares se comunican e incorporan a la capacitación y las desviaciones son monitoreadas, rastreadas y reportadas. Se utilizan herramientas automatizadas para fomentar el uso de estándares y mejorar la estabilidad. Los sistemas de administración de configuraciones cubren la mayoría de los activos de TI y permiten una adecuada administración de liberaciones y control de distribución. Los análisis de excepciones, así como las verificaciones físicas, se aplican de manera consistente y se investigan las causas desde su raíz.		**X**	
5 Optimizado cuando Todos los activos de TI se administran en un sistema central de configuraciones que contiene toda la información necesaria acerca de los componentes, sus interrelaciones y eventos. La información de las configuraciones está alineada con los catálogos de los proveedores. Hay una completa integración de los procesos interrelacionados, y estos utilizan y actualizan la información de la configuración de manera automática. Los reportes de auditoría de los puntos de referencia, brindan información esencial sobre el software con respecto a reparaciones, servicios, garantías, actualizaciones y evaluaciones técnicas de cada unidad individual. Se fomentan las reglas para limitar la instalación de software no autorizado. La gerencia proyecta las reparaciones y las actualizaciones utilizando reportes de análisis que proporcionan funciones de programación de actualizaciones y de renovación de tecnología. El rastreo de activos y el monitoreo de activos individuales de TI los protege y previene de robo, de mal uso y de abusos.		**X**	

Tabla 32: MODELOS DE MADUREZ DS9

Fuente: Realizado por el autor

DOMINIO: ENTREGAR Y DAR SOPORTE **DS10: Administración de problemas**			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de administración de problemas se encuentra en el nivel 3.
0 No existente cuando No hay conciencia sobre la necesidad de administrar problemas, y no hay diferencia entre problemas e incidentes. Por lo tanto, no se han hecho intentos por identificar la causa raíz de los incidentes.	**X**		
1 Inicial/Ad Hoc cuando Los individuos reconocen la necesidad de administrar los problemas y de revolver las causas de fondo. Algunos individuos expertos clave brindan asesoría sobre problemas relacionados a su área de experiencia, pero no está asignada la responsabilidad para la administración de problemas. La información no se comparte, resultando en la creación de nuevos problemas y la pérdida de tiempo productivo mientras se buscan respuestas.	**X**		

2 Repetible pero intuitiva cuando Hay una amplia conciencia sobre la necesidad y los beneficios de administrar los problemas relacionados con TI, tanto dentro de las áreas de negocio como en la función de servicios de información. El proceso de resolución ha evolucionado un punto en el que unos cuantos individuos clave son responsables de identificar y resolver los problemas. La información se comparte entre el personal de manera informal y reactiva. El nivel de servicio hacia la comunidad usuaria varía y es obstaculizado por la falta de conocimiento estructurado a disposición del administrador de problemas.	**X**		
3 Proceso definido cuando Se acepta la necesidad de un sistema integrado de administración de problemas y se evidencia con el apoyo de la gerencia y la asignación de presupuesto para personal y capacitación. Se estandarizan los procesos de escalamiento y resolución de problemas. El registro y rastreo de problemas y de sus soluciones se dividen dentro del equipo de respuesta, utilizando las herramientas disponibles sin centralizar. Es poco probable detectar las desviaciones de los estándares y de las normas establecidas. La información se comparte entre el personal de manera formal y proactiva. La revisión de incidentes y los análisis de identificación y resolución de problemas son limitados e informales.		**X**	
4 Administrado y medible cuando Se acepta la necesidad de un sistema integrado de administración de problemas y se evidencia con el apoyo de la gerencia y la asignación de presupuesto para personal y capacitación. Se estandarizan los procesos de escalamiento y resolución de problemas. El registro y rastreo de problemas y de sus soluciones se dividen dentro del equipo de respuesta, utilizando las herramientas disponibles sin centralizar. Es poco probable detectar las desviaciones de los estándares y de las normas establecidas. La información se comparte entre el personal de manera formal y proactiva. La revisión de incidentes y los análisis de identificación y resolución de problemas son limitados e informales.		**X**	
5 Optimizado cuando El proceso de administración de problemas ha evolucionado a un proceso proactivo y preventivo, que contribuye con los objetivos de TI. Los problemas se anticipan y previenen. El conocimiento respecto a patrones de problemas pasados y futuros se mantiene a través de contactos regulares con proveedores y expertos. El registro, reporte y análisis de problemas y soluciones está integrado por completo con la administración de datos de configuración. Los KPIs y KGIs son medidos de manera consistente. La mayoría de los sistemas están equipados con mecanismos automáticos de advertencia y detección, los cuales son rastreados y evaluados de manera continua. El proceso de administración de problemas se analiza para buscar la mejora continua con base en los KPIs y KGIs y se reporta a los interesados.		**X**	

Tabla 33: MODELOS DE MADUREZ DS10

Fuente: Realizado por el autor

DOMINIO: ENTREGAR Y DAR SOPORTE **DS11: Administración de datos**			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de administración de datos se encuentra en el nivel 2.
0 No existente cuando Los datos no son reconocidos como parte de los recursos y los activos de la empresa. No está asignada la propiedad sobre los datos o sobre la rendición de cuentas individual sobre la administración de los datos. La calidad y la seguridad de los datos son deficientes o inexistentes.	**X**		

1 Inicial/Ad Hoc cuando La organización reconoce la necesidad de una correcta administración de los datos. Hay un método adecuado para especificar requerimientos de seguridad en la administración de datos, pero no hay procedimientos implementados de comunicación formal. No se lleva a cabo capacitación específica sobre administración de los datos. La responsabilidad sobre la administración de los datos no es clara. Los procedimientos de respaldo y recuperación y los acuerdos sobre desechos están en orden.	**X**		
2 Repetible pero intuitiva cuando A lo largo de toda la organización existe conciencia sobre la necesidad de una adecuada administración de los datos. A un alto nivel empieza a observarse la propiedad o responsabilidad sobre los datos. Los requerimientos de seguridad para la administración de datos son documentados por individuos clave. Se lleva a cabo algún tipo de monitoreo dentro de TI sobre algunas actividades clave de la administración de datos (respaldos, recuperación y desecho). Las responsabilidades para la administración de datos son asignadas de manera informal a personal clave de TI.		**X**	
3 Proceso definido cuando Se entiende y acepta la necesidad de la administración de datos, tanto dentro de TI como a lo largo de toda la organización. Se establece la responsabilidad sobre la administración de los datos. Se asigna la propiedad sobre los datos a la parte responsable que controla la integridad y la seguridad. Los procedimientos de administración de datos se formalizan dentro de TI y se utilizan algunas herramientas para respaldos / recuperación y desecho de equipo. Se lleva a cabo algún tipo de monitoreo sobre la administración de datos. Se definen métricas básicas de desempeño. Comienza a aparecer el entrenamiento sobre administración de información.		**X**	
4 Administrado y medible cuando Se entiende la necesidad de la administración de los datos y las acciones requeridas son aceptadas a lo largo de toda la organización. La responsabilidad de la propiedad y la administración de los datos están definidas, asignada y comunicada de forma clara en la organización. Los procedimientos se formalizan y son ampliamente conocidos, el conocimiento se comparte. Comienza a aparecer el uso de herramientas. Se acuerdan con los clientes los indicadores de desempeño y meta y se monitorean por medio de un proceso bien definido. Se lleva a cabo entrenamiento formal para el personal de administración de los datos.		**X**	
5 Optimizado cuando Se entiende y acepta dentro de la organización la necesidad de realizar todas las actividades requeridas para la administración de datos. Las necesidades y los requerimientos futuros son explorados de manera proactiva. Las responsabilidades sobre la propiedad de los datos y la administración de los mismos están establecidas de forma clara, se conocen ampliamente a lo largo de la organización y se actualizan periódicamente. Los procedimientos se formalizan y se conocen ampliamente, la compartición del conocimiento es una práctica estándar. Se utilizan herramientas sofisticadas con un máximo de automatización de la administración de los datos. Se acuerdan con los clientes los indicadores de desempeño y meta, se ligan con los objetivos del negocio y se monitorean de manera regular utilizando un proceso bien definido. Se exploran constantemente oportunidades de mejora. El entrenamiento para el personal de administración de datos se institucionaliza.		**X**	

Tabla 34: MODELOS DE MADUREZ DS11

Fuente: Realizado por el autor

DOMINIO: ENTREGAR Y DAR SOPORTE DS12: Administración del ambiente físico			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de administración del ambiente físico se encuentra en el nivel 3.
0 No existente cuando No hay conciencia sobre la necesidad de proteger las instalaciones o la inversión en recursos de cómputo. Los factores ambientales tales como protección contra fuego, polvo, tierra y exceso de calor y humedad no se controlan ni se monitorean.	**X**		
1 Inicial/Ad Hoc cuando La organización reconoce la necesidad de contar con un ambiente físico que proteja los recursos y el personal contra peligros naturales y causados por el hombre. La administración de instalaciones y de equipo depende de las habilidades de individuos clave. El personal se puede mover dentro de las instalaciones sin restricción. La gerencia no monitorea los controles ambientales de las instalaciones o el movimiento del personal.	**X**		
2 Repetible pero intuitiva cuando Los controles ambientales se implementan y monitorean por parte del personal de operaciones. La seguridad física es un proceso informal, realizado por un pequeño grupo de empleados con alto nivel de preocupación por asegurar las instalaciones físicas. Los procedimientos de mantenimiento de instalaciones no están bien documentados y dependen de las buenas prácticas de unos cuantos individuos. Las metas de seguridad física no se basan en estándares formales y la gerencia no se asegura de que se cumplan los objetivos de seguridad.	**X**		
3 Proceso definido cuando Se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de cómputo controlado. Los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con presupuesto autorizado y rastreado por la gerencia. Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado. Los visitantes se registran y acompañan dependiendo del individuo. Las instalaciones físicas mantienen un perfil bajo y no son reconocibles de manera fácil. Las autoridades civiles monitorean al cumplimiento con los reglamentos de salud y seguridad. Los riesgos se aseguran con el mínimo esfuerzo para optimizar los costos del seguro.		**X**	
4 Administrado y medible cuando Se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de cómputo controlado. Los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con presupuesto autorizado y rastreado por la gerencia. Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado. Los visitantes se registran y acompañan dependiendo del individuo. Las instalaciones físicas mantienen un perfil bajo y no son reconocibles de manera fácil. Las autoridades civiles monitorean al cumplimiento con los reglamentos de salud y seguridad. Los riesgos se aseguran con el mínimo esfuerzo para optimizar los costos del seguro.		**X**	
5 Optimizado cuando Se entiende por completo la necesidad de mantener un ambiente de cómputo controlado y se evidencia en la estructura organizacional y en la distribución del presupuesto. Los requerimientos de seguridad físicos y ambientales están documentados y el acceso se monitorea y controla estrictamente. Se establecen y comunican las responsabilidades. El personal de las instalaciones ha sido entrenado por completo respecto a situaciones de emergencia, así como en prácticas de salud y seguridad. Están implementados mecanismos de control estandarizados para la restricción de accesos a instalaciones y para contrarrestar los factores ambientales y de seguridad. La gerencia monitorea la efectividad de los controles y el cumplimiento de los estándares establecidos. La gerencia ha establecido KPIs y KGIs para medir la administración del ambiente de cómputo. La capacidad de recuperación de los recursos de cómputo se incorpora en un proceso organizacional de administración de riesgos. La información integrada se usa para optimizar la cobertura de los seguros y de los costos asociados.		**X**	

Tabla 35: MODELOS DE MADUREZ DS12

Fuente: Realizado por el autor

DOMINIO: ENTREGAR Y DAR SOPORTE DS13: Administración de operaciones			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de administración de operaciones se encuentra en el nivel 2.
0 No existente cuando La organización no dedica tiempo y recursos al establecimiento de soporte básico de TI y a actividades operativas.	**X**		
1 Inicial/Ad Hoc cuando La organización reconoce la necesidad de estructurar las funciones de soporte de TI. Se establecen algunos procedimientos estándar y las actividades de operaciones son de naturaleza reactiva. La mayoría de los procesos de operación son programados de manera informal y el procesamiento de peticiones se acepta sin validación previa. Las computadoras, sistemas y aplicaciones que soportan los procesos del negocio con frecuencia no están disponibles, se interrumpen o retrasan. Se pierde tiempo mientras los empleados esperan recursos. Los medios de salida aparecen ocasionalmente en lugares inesperados o no aparecen.		**X**	
2 Repetible pero intuitiva cuando La organización esta consiente del rol clave que las actividades de operaciones de TI juegan en brindar funciones de soporte de TI. Se asignan presupuestos para herramientas con un criterio de caso por caso. Las operaciones de soporte de TI son informales e intuitivas. Hay una alta dependencia sobre las habilidades de los individuos. Las instrucciones de qué hacer, cuándo y en qué orden no están documentadas. Existe algo de capacitación para el operador y hay algunos estándares de operación formales.		**X**	
3 Proceso definido cuando Se entiende y acepta dentro de la organización la necesidad de administrar las operaciones de cómputo. Se han asignado recursos y se lleva a cabo alguna capacitación durante el trabajo. Las funciones repetitivas están definidas, estandarizadas, documentadas y comunicadas de manera formal. Los resultados de las tareas completadas y de los eventos se registran, con reportes limitados hacia la gerencia. Se introduce el uso de herramientas de programación automatizadas y de otras herramientas para limitar la intervención del operador. Se introducen controles para colocar nuevos trabajos en operación. Se desarrolla una política formal para reducir el número de eventos no programados. Los acuerdos de servicio y mantenimiento con proveedores siguen siendo de naturaleza informal.		**X**	
4 Administrado y medible cuando Se entiende y acepta dentro de la organización la necesidad de administrar las operaciones de cómputo. Se han asignado recursos y se lleva a cabo alguna capacitación durante el trabajo. Las funciones repetitivas están definidas, estandarizadas, documentadas y comunicadas de manera formal. Los resultados de las tareas completadas y de los eventos se registran, con reportes limitados hacia la gerencia. Se introduce el uso de herramientas de programación automatizadas y de otras herramientas para limitar la intervención del operador. Se introducen controles para colocar nuevos trabajos en operación. Se desarrolla una política formal para reducir el número de eventos no programados. Los acuerdos de servicio y mantenimiento con proveedores siguen siendo de naturaleza informal.		**X**	
5 Optimizado cuando Las operaciones de soporte de TI son efectivas, eficientes y suficientemente flexibles para cumplir con las necesidades de niveles de servicio con una pérdida de productividad mínima. Los procesos de administración de operaciones de TI están estandarizados y documentados en una base de conocimiento, y están sujetos a una mejora continua. Los procesos automatizados que soportan los sistemas contribuyen a un ambiente estable. Todos los problemas y fallas se analizan para identificar la causa que los originó. Las reuniones periódicas con los responsables de administración del cambio garantizan la inclusión oportuna de cambios en las programaciones de producción. En colaboración con los proveedores, el equipo se analiza respecto a posibles síntomas de obsolescencia y fallas, y el mantenimiento es principalmente de naturaleza preventiva.		**X**	

Tabla 36: MODELOS DE MADUREZ DS13

DOMINIO: MONITOREAR Y EVALUAR ME1: Monitorear y evaluar el desempeño de TI			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de Monitorear y evaluar el desempeño de TI se encuentra en el nivel 3.
0 No existente cuando La organización no cuenta con un proceso implantado de monitoreo. TI no lleva a cabo monitoreo de proyectos o procesos de forma independiente. No se cuenta con reportes útiles, oportunos y precisos. La necesidad de entender de forma clara los objetivos de los procesos no se reconoce.	**X**		
1 Inicial/Ad Hoc cuando La gerencia reconoce una necesidad de recolectar y evaluar información sobre los procesos de monitoreo. No se han identificado procesos estándar de recolección y evaluación. El monitoreo se implanta y las métricas se seleccionan de acuerdo a cada caso, de acuerdo a las necesidades de proyectos y procesos de TI específicos. El monitoreo por lo general se implanta de forma reactiva a algún incidente que ha ocasionado alguna perdida o vergüenza a la organización. La función de contabilidad monitorea mediciones financieras básicas para TI.	**X**		
2 Repetible pero intuitiva cuando Se han identificado algunas mediciones básicas a ser monitoreadas. Los métodos y las técnicas de recolección y evaluación existen, pero los procesos no se han adoptado en toda la organización. La interpretación de los resultados del monitoreo se basa en la experiencia de individuos clave. Herramientas limitadas son seleccionadas y se implantan para recolectar información, pero esta recolección no se basa en un enfoque planeado.	**X**		
3 Proceso definido cuando La gerencia ha comunicado e institucionalizado un procesos estándar de monitoreo. Se han implantado programas educacionales y de entrenamiento para el monitoreo. Se ha desarrollado una base de conocimiento formalizada del desempeño histórico. Las evaluaciones todavía se realizan al nivel de procesos y proyectos individuales de TI y no están integradas a través de todos los procesos. Se han definido herramientas para monitorear los procesos y los niveles de servicio de TI. Las mediciones de la contribución de la función de servicios de información al desempeño de la organización se han definido, usando criterios financieros y operativos tradicionales. Las mediciones del desempeño específicas de TI, las mediciones no financieras, las estratégicas, las de satisfacción del cliente y los niveles de servicio están definidas. Se ha definido un marco de trabajo para medir el desempeño.		**X**	
4 Administrado y medible cuando La gerencia ha definido las tolerancias bajo las cuales los procesos deben operar. Los reportes de los resultados del monitoreo están en proceso de estandarizarse y normalizarse. Hay una integración de métricas a lo largo de todos los proyectos y procesos de TI. Los sistemas de reporte de la administración de TI están formalizados. Las herramientas automatizadas están integradas y se aprovechan en toda la organización para recolectar y monitorear la información operativa de las aplicaciones, sistemas y procesos. La gerencia puede evaluar el desempeño con base en criterios acordados y aprobados por las terceras partes interesadas. Las mediciones de la función de TI están alienadas con las metas de toda la organización.		**X**	
5 Optimizado cuando Un proceso de mejora continua de la calidad se ha desarrollado para actualizar los estándares y las políticas de monitoreo a nivel organizacional incorporando mejores prácticas de la industria. Todos los procesos de monitoreo están optimizados y dan soporte a los objetivos de toda la organización. Las métricas impulsadas por el negocio se usan de forma rutinaria para medir el desempeño, y están integradas en los marcos de trabajo estratégicos, tales como el Balanced Scorecard. El monitoreo de los procesos y el rediseño continuo son consistentes con los planes de mejora de los procesos de negocio en toda la organización. Benchmarks contra la industria y los competidores clave se han formalizado, con criterios de comparación bien entendidos.		**X**	

Tabla 37: MODELOS DE MADUREZ ME1

DOMINIO: MONITOREAR Y EVALUAR ME2: Monitorear y evaluar el control interno			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	**GRADO DE MADUREZ.** El proceso de monitorear y evaluar el control interno se encuentra en el nivel 2.
0 No existente cuando La organización carece de procedimientos para monitorear la efectividad de los controles internos. Los métodos de reporte de control interno gerenciales no existen. Existe una falta generalizada de conciencia sobre la seguridad operativa y el aseguramiento del control interno de TI. La gerencia y los empleados no tienen conciencia general sobre el control interno.	**X**		
1 Inicial/Ad Hoc cuando La gerencia reconoce la necesidad de administrar y asegurar el control de TI de forma regular. La experiencia individual para evaluar la suficiencia del control interno se aplica de forma ad hoc. La gerencia de TI no ha asignado de manera formal las responsabilidades para monitorear la efectividad de los controles internos. Las evaluaciones de control interno de TI se realizan como parte de las auditorías financieras tradicionales, con metodologías y habilidades que no reflejan las necesidades de la función de los servicios de información.	**X**		
2 Repetible pero intuitiva cuando La organización utiliza reportes de control informales para comenzar iniciativas de acción correctiva. La evaluación del control interno depende de las habilidades de individuos clave. La organización tiene una mayor conciencia sobre el monitoreo de los controles internos. La gerencia de servicios de información realiza monitoreo periódico sobre la efectividad de lo que considera controles internos críticos. Se están empezando a usar metodologías y herramientas para monitorear los controles internos, aunque no se basan en un plan. Los factores de riesgo específicos del ambiente de TI se identifican con base en las habilidades de individuos.		**X**	
3 Proceso definido cuando La gerencia apoya y ha institucionalizado el monitoreo del control interno. Se han desarrollado políticas y procedimientos para evaluar y reportar las actividades de monitoreo del control interno. Se ha definido un programa de educación y entrenamiento para el monitoreo del control interno. Se ha definido también un proceso para auto-evaluaciones y revisiones de aseguramiento del control interno, con roles definidos para los responsables de la administración del negocio y de TI. Se usan herramientas, aunque no necesariamente están integradas en todos los procesos. Las políticas de evaluación de riesgos de los procesos de TI se utilizan dentro de los marcos de trabajo desarrollados de manera específica para la función de TI. Se han definido políticas para el manejo y mitigación de riesgos específicos de procesos.		**X**	
4 Administrado y medible cuando La gerencia tiene implantado un marco de trabajo para el monitoreo del control interno de TI. La organización ha establecido niveles de tolerancia para el proceso de monitoreo del control interno. Se han implantado herramientas para estandarizar evaluaciones y para detectar de forma automática las excepciones de control. Se ha establecido una función formal para el control interno de TI, con profesionales especializados y certificados que utilizan un marco de trabajo de control formal avalado por la alta dirección. Un equipo calificado de TI participa de forma rutinaria en las evaluaciones de control interno. Se ha establecido una base de datos de métricas para información histórica sobre el monitoreo del control interno. Se realizan revisiones entre pares para verificar el monitoreo del control interno.		**X**	
5 Optimizado cuando La gerencia ha implantado un programa de mejora continua en toda la organización que toma en cuenta las lecciones aprendidas y las mejores prácticas de la industria para monitorear el control interno. La organización utiliza herramientas integradas y actualizadas, donde es apropiado, que permiten una evaluación efectiva de los controles críticos de TI y una detección rápida de incidentes de control de TI. La compartición del conocimiento, específico de la función de servicios de información, se encuentra implantada de manera formal. El benchmarking con los estándares de la industria y las mejores prácticas está formalizado.		**X**	

Tabla 38: MODELOS DE MADUREZ ME2

Fuente: Realizado por el autor

DOMINIO: MONITOREAR Y EVALUAR ME3: Garantizar el cumplimiento regulatorio			
Niveles	**Cumple**		**Observaciones**
	SI	**NO**	
0 No existente cuando Existe poca conciencia respecto a los requerimientos externos que afectan a TI, sin procesos referentes al cumplimiento de requisitos regulatorios, legales y contractuales.	**X**	**X**	**GRADO DE MADUREZ.** El proceso de garantizar el Cumplimiento regulatorio se encuentra en el nivel 3.
1 Inicial/Ad Hoc cuando Existe conciencia de los requisitos de cumplimiento regulatorio, contractual y legal que tienen impacto en la organización. Se siguen procesos informales para mantener el cumplimiento, pero solo si la necesidad surge en nuevos proyectos o como respuesta a auditorías o revisiones.		**X**	
2 Repetible pero intuitiva cuando Existe el entendimiento de la necesidad de cumplir con los requerimientos externos y la necesidad se comunica. En los casos en que el cumplimiento se ha convertido en un requerimiento recurrente., como en los reglamentos regulatorios o en la legislación de privacidad, se han desarrollado procedimientos individuales de cumplimiento y se siguen año con año. No existe, sin embargo, un enfoque estándar. Hay mucha confianza en el conocimiento y responsabilidad de los individuos, y los errores son posibles. Se brinda entrenamiento informal respecto a los requerimientos externos y a los temas de cumplimiento.		**X**	
3 Proceso definido cuando Se han desarrollado, documentado y comunicado políticas, procedimientos y procesos, .para garantizar el cumplimiento de los reglamentos y de las obligaciones contractuales y legales, pero algunas quizá no se sigan y algunas quizá estén desactualizadas o sean poco prácticas de implantar. Se realiza poco monitoreo y existen requisitos de cumplimiento que no han sido resueltos. Se brinda entrenamiento sobre requisitos legales y regulatorios externos que afectan a la organización y se instruye respecto a los procesos de cumplimiento definidos. Existen contratos pro forma y procesos legales estándar para minimizar los riesgos asociados con las obligaciones contractuales		**X**	
4 Administrado y medible cuando Existe un entendimiento completo de los eventos y de la exposición a requerimientos externos, y la necesidad de asegurar el cumplimiento a todos los niveles. Existe un esquema formal de entrenamiento que asegura que todo el equipo esté consciente de sus obligaciones de cumplimiento. Las responsabilidades son claras y el empoderamiento de los procesos es entendido. El proceso incluye una revisión del entorno para identificar requerimientos externos y cambios recurrentes. Existe un mecanismo implantado para monitorear el no cumplimiento de los requisitos externos, reforzar las prácticas internas e implantar acciones correctivas. Los eventos de no cumplimiento se analizan de forma estándar en busca de las causas raíz, con el objetivo de identificar soluciones sostenibles. Buenas prácticas internas estandarizadas se usan para necesidades específicas tales como reglamentos vigentes y contratos recurrentes de servicio.		**X**	
5 Optimizado cuando Existe un proceso bien organizado, eficiente e implantado para cumplir con los requerimientos externos, basado en una sola función central que brinda orientación y coordinación a toda la organización. Hay un amplio conocimiento de los requerimientos externos aplicables, incluyendo sus tendencias futuras y cambios anticipados, así como la necesidad de nuevas soluciones. La organización participa en discusiones externas con grupos regulatorios y de la industria para entender e		**X**	

influenciar los requerimientos externos que la puedan afectar. Se han desarrollado mejores prácticas que aseguran el cumplimiento de los requisitos externos, y esto ocasiona que haya muy pocos casos de excepciones de cumplimiento. Existe un sistema central de rastreo para toda la organización, que permite a la gerencia documentar el flujo de trabajo, medir y mejorar la calidad y efectividad del proceso de monitoreo del cumplimiento. Un proceso externo de auto-evaluación de requerimientos existe y se ha refinado hasta alcanzar el nivel de buena práctica. El estilo y la cultura administrativa de la organización referente al cumplimiento es suficientemente fuerte, y se elaboran los procesos suficientemente bien para que el entrenamiento se limite al nuevo personal y siempre que ocurra un cambio significativo.			

Tabla 39: MODELOS DE MADUREZ ME3

Fuente: Realizado por el autor

3.3. Reporte general de modelos de madurez

La siguiente tabla (Tabla 40) muestra el reporte del grado de madurez de cada proceso evaluado, se puede observar que hay procesos con grado de madurez 1 o inicial que deben ser motivo de especial atención por parte del departamento, como plan a corto plazo.

DOMINIO	PROCESO		GRADO DE MADUREZ
Planear y Organizar	PO1	Definir un plan estratégico de TI	3
	PO2	Definir la Arquitectura de la Información	2
	PO3	Definir la dirección tecnológica	3
	PO4	Definir los Procesos, Organización y Relaciones de TI	3
	PO5	Administrar la Inversión en TI	1
	PO6	Comunicar las metas y la dirección de la gerencia	3
	PO7	Administrar los Recursos Humanos de TI	3
	PO9	Evaluar y Administrar los Riesgos de TI	2
	PO10	Administrar los proyectos	2
Adquirir e Implantar	AI1	Identificar las Soluciones Automatizadas	3
	AI2	Adquirir y Mantener Software Aplicativo	3
	AI3	Adquirir y Mantener la Infraestructura Tecnológica	3
	AI4	Facilitar la operación y el uso	3
	AI5	Procurar Recursos de TI	1
	AI6	Administrar los Cambios	1
	AI7	Instalar y Acreditar soluciones y cambios	3

Entregar y Dar Soporte	DS2	Administrar los Servicios de Terceros	3
	DS3	Administrar el Desempeño y la Capacidad	2
	DS4	Asegurar el Servicio Continuo	2
	DS5	Garantizar la Seguridad de los Sistemas	2
	DS7	Educar y Entrenar a los Usuarios	2
	DS8	Administrar la mesa de Servicio y los Incidentes	2
	DS9	Administrar la Configuración	2
	DS10	Administrar los Problemas	3
	DS11	Administrar los Datos	2
	DS12	Administrar el Ambiente Físico	3
	DS13	Administrar las Operaciones	2
Monitorear y Evaluar	ME1	Monitorear y evaluar el desempeño de TI	3
	ME2	Monitorear y evaluar el Control Interno	2
	ME3	Garantizar el cumplimiento Regulatorio	3

Tabla 40: Reporte general de modelos de madurez

Fuente: Creado por el autor

3.4. Resultados finales del impacto sobre los criterios de información

Los resultados presentados en la siguiente tabla (Tabla 41) resultan de la multiplicación entre el valor propuesto por COSO (Tabla 9) para cada criterio y el valor obtenido del grado de madurez (Tabla 40) en que se encuentra cada proceso relacionado con la situación actual. Se obtiene el total real haciendo una sumatoria por cada columna de criterios; el cual se lo compara con el total ideal que resulta de la suma por columna si se considera que el grado de madurez de cada criterio es óptimo 5.Posteriormente se realiza el cálculo del porcentaje dividiendo el total real para el total ideal y multiplicando por 100. Finalmente se obtiene el promedio de los porcentajes de los criterios de información.

DOMINIO	PROCESO		EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD
Planear y Organizar	PO1	Definir un plan estratégico de	**2,58**	**1,89**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
	PO2	Definir la Arquitectura de la Información	**1,89**	**1,72**	**0,40**	**0,74**	**0,00**	**0,00**	**0,00**
	PO3	Definir la dirección tecnológica	**2,58**	**2,58**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
	PO4	Definir los Procesos, Organización y Relaciones de TI	**2,58**	**2,58**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
	PO5	Administrar la Inversión en TI	**2,58**	**0,86**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
	PO6	Comunicar las metas y la dirección de la gerencia	**2,58**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
	PO7	Administrar los Recursos Humanos de TI	**2,58**	**2,58**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
	PO9	Evaluar y Administrar los Riesgos de TI	**1,89**	**1,26**	**0,54**	**0,54**	**0,74**	**0,54**	**0,54**
	PO10	Administrar los proyectos	**2,58**	**1,72**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
Adquirir e Implantar	AI1	Identificar las Soluciones Automatizadas	**2,58**	**1,89**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
	AI2	Adquirir y Mantener Software Aplicativo	**2,58**	**2,58**	**0,00**	**0,54**	**0,00**	**0,00**	**0,00**

	AI3	Adquirir y Mantener la Infraestructura Tecnológica	**1,89**	**2,58**	**0,00**	**0,54**	**0,00**	**0,00**	**0,00**
	AI4	Facilitar la operación y el uso	**2,58**	**2,58**	**0,00**	**0,54**	**0,00**	**0,40**	**0,40**
	AI5	Procurar Recursos de TI	**1,89**	**0,89**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
	AI6	Administrar los Cambios	**2,58**	**0,86**	**0,00**	**0,74**	**0,00**	**0,00**	**0,54**
	AI7	Instalar y Acreditar soluciones y cambios	**2,58**	**1,89**	**0,00**	**0,40**	**0,00**	**0,00**	**0,00**
Entregar y dar Soporte	DS2	Administrar los Servicios de Terceros	**2,58**	**2,58**	**0,54**	**0,54**	**0,40**	**0,40**	**0,40**
	DS3	Administrar el Desempeño y la Capacidad	**2,58**	**1,72**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
	DS4	Asegurar el Servicio Continuo	**2,58**	**1,26**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
	DS5	Garantizar la Seguridad de los Sistemas	**0,00**	**0,00**	**0,00**	**0,00**	**0,54**	**0,54**	**0,40**
	DS7	Educar y Entrenar a los Usuarios	**2,58**	**1,26**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
	DS8	Administrar la mesa de Servicio y los Incidentes	**2,58**	**1,72**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
	DS9	Administrar la Configuración	**2,58**	**1,26**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
	DS10	Administrar los Problemas	**2,58**	**2,58**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
	DS11	Administrar los Datos	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
	DS12	Administrar el Ambiente Físico	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**

	DS13	Administrar las Operaciones	**2,58**	**1,72**	**0,00**	**0,54**	**0,00**	**0,00**	**0,00**
Monitorear y Evaluar	ME1	Monitorear y evaluar el desempeño de TI	**2,58**	**2,58**	**0,54**	**0,54**	**0,40**	**0,40**	**0,40**
	ME2	Monitorear y evaluar el Control Interno	**2,58**	**1,72**	**0,54**	**0,54**	**0,40**	**0,40**	**0,40**
	ME3	Garantizar el cumplimiento Regulatorio	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
		TOTAL REAL	**64,32**	**46,83**	**2,56**	**6,21**	**2,47**	**2,67**	**3,47**
		TOTAL IDEAL	**107,20**	**99,45**	**21,20**	**51,00**	**51,85**	**29,50**	**38,95**
		PORCENTAJE	**60.00%**	**47.09%**	**12.09%**	**12.18%**	**4.77%**	**9.05%**	**8.90%**
PROMEDIO DE CRITERIOS DE INFORMACION			**22.01%**						

Tabla 41: Resumen de procesos y criterios de información por impacto.

FUENTE: Realizado por el autor

3.5. Grafica representativa del impacto de los criterios de información

En la siguiente gráfica (Figura 4) se observa el resultado de los porcentajes obtenidos en la Tabla 41, que da una idea de cómo en el Departamento los procesos impactan a cada uno de los criterios de información.

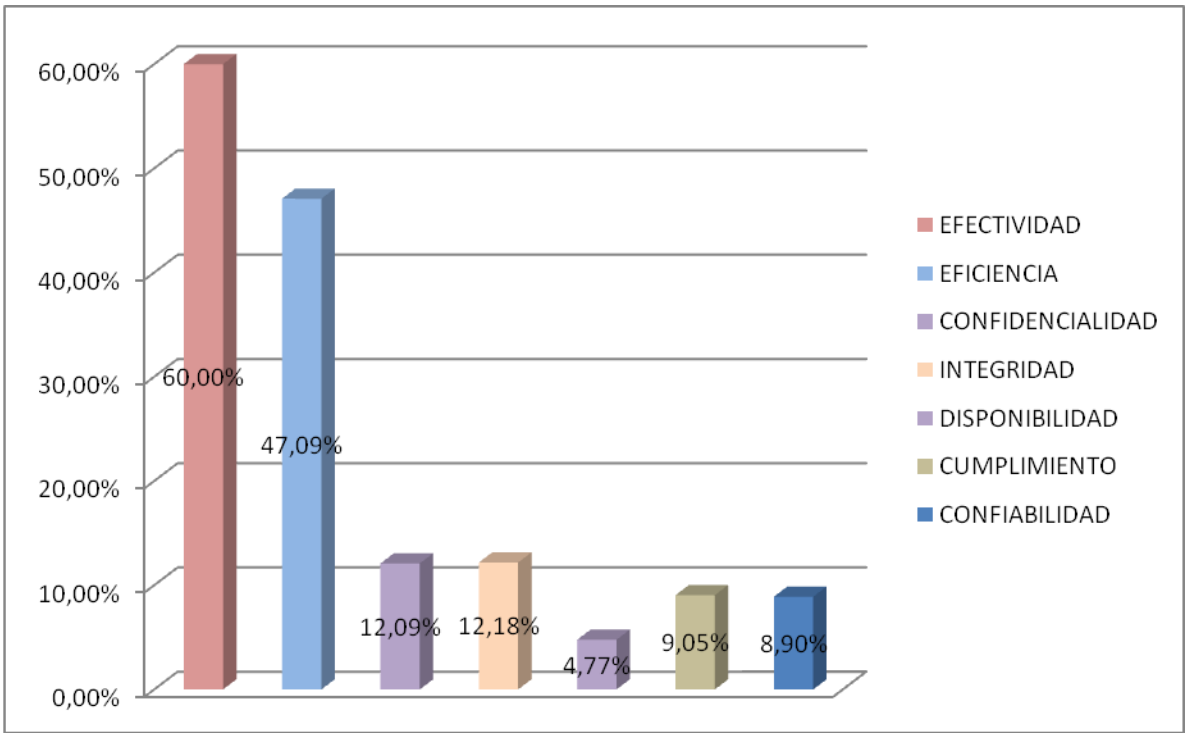

Figura 4: Criterios de Información

FUENTE: Realizado por el autor

4.- Presentación de resultados

4.1. Elaboración del informe final

A continuación se presenta el Informe de los procesos establecidos por COBIT (Tabla 42 a Tabla 71) aplicados al departamento, presentando para cada uno el factor de riesgo y las recomendaciones respectivas.

PO1: Definir el plan estratégico de TI	Grado de Madurez 3
FACTOR DE RIESGO: No hay una política que defina como y cuando realizar la planeación estratégica de TI. La planeación estratégica de TI no sigue un enfoque estructurado, en el que se documente y de a conocer a todo el equipo. El proceso de planeación de TI no es sólido y no garantiza que es factible realizar una planeación adecuada. La estrategia general de TI no incluye una definición consistente de los riesgos que la organización está dispuesta a tomar como innovador o como seguidor[9]. Las estrategias de recursos humanos, técnicos y financieros de TI no influencian la adquisición de nuevos productos y tecnologías.	
RECOMENDACIONES COBIT: ➢ Elaborar el Plan Estratégico de TI con la intervención de las gerencias y teniendo en cuenta las necesidades actuales y futuras. ➢ Analizar y entender las capacidades actuales del Departamento de TI. ➢ Aplicar un esquema de prioridades para los objetivos del negocio que cuantifique los requerimientos del Departamento.	

Tabla 42: Resumen de resultados PO1

Fuente: Creado por el autor

[9] Seguidor: Que se fomente seguir el Plan Estratégico para mejorar la situación de la empresa.
Fuente: Los autores.

PO2: Definir la arquitectura de la información	Grado de Madurez 2
FACTOR DE RIESGO: No hay un proceso de arquitectura de información ni procedimientos similares, ni intuitivos o informales. Las personas obtienen sus habilidades al construir la arquitectura de información por medio de experiencia práctica y la aplicación repetida de técnicas.	
RECOMENDACIONES COBIT: ➢ Elaborar la arquitectura de la información y datos asignando la propiedad de los mismos para garantizar el correcto uso y seguridad de la información. ➢ Usar un esquema de clasificación de la información acordado.	

Tabla 43: Resumen de resultados PO2

Fuente: Creado por el autor

PO3: Determinar la dirección tecnológica	Grado de Madurez 3
FACTOR DE RIESGO: La gerencia no está totalmente consciente de la importancia del plan de infraestructura tecnológica. No hay un plan de infraestructura tecnológica definido, documentado y difundido. Los proveedores clave no se seleccionan con base en su entendimiento de la tecnología a largo plazo y de los planes de desarrollo de productos.	
RECOMENDACIONES COBIT: ➢ Establecer la arquitectura de la información estableciendo un foro para dirigir la arquitectura y verificar el cumplimiento ➢ Establecer un Plan de Infraestructura tecnológica equilibrando costos, riesgos y requerimientos y basándose en las necesidades de la arquitectura de la información.	

Tabla 44: Resumen de resultados PO3

Fuente: Creado por el autor

PO4: Definir procesos, organización y relaciones de TI	Grado de Madurez 3
FACTOR DE RIESGO: Existen roles y responsabilidades definidos para la organización de TI. La organización de TI no desarrolla, documenta, comunica y se alinea con la estrategia de TI. No se formulan las relaciones con terceros, incluyendo los comités de dirección, auditoría interna y administración de proveedores. La organización de TI no está funcionalmente completa. Existen definiciones de las funciones a ser realizadas por parte del personal de TI y las que deben realizar los usuarios pero no están bien definidos ya que en ciertas ocasiones todos realizan las mismas funciones por la falta de personal para cubrir las necesidades del momento. No hay una definición formal de las relaciones con los usuarios y con terceros. La división de roles y responsabilidades no está bien definida e implantada.	
RECOMENDACIONES COBIT: ➢ Establecer los procesos de TI y de la empresa en general y establecer roles y responsabilidades de las personas que intervienen o intervendrán en la ejecución de dichos propósitos. ➢ Establecer una estructura organizacional apropiada colocando al Departamento de TI en el nivel que le corresponde por las actividades que realiza, que es nivel asesor para que el mismo tenga poder de decisión dentro de Agua de los Andes S.A.	

Tabla 45: Resumen de resultados PO4

Fuente: Creado por el autor

PO5: Administrar la inversión en TI	Grado de Madurez 1
FACTOR DE RIESGO: La organización no reconoce en su totalidad la necesidad de administrar la inversión en TI, y lo poco que reconoce se comunica de manera inconsistente. La asignación de responsabilidades de selección de inversiones en TI y de desarrollo de presupuestos se hace de una forma inicial. Existen implantaciones aisladas de selección y presupuesto de inversiones en TI, con documentación informal. Las inversiones en TI se justifican de manera informal. Se toman decisiones presupuestales enfocadas de modo reactivo y operativo.	
RECOMENDACIONES COBIT: ➢ Tomar conciencia de que la información o datos del Departamento son un activo más, para la adecuada asignación de presupuesto. ➢ Definir criterios formales de inversión. ➢ Medir y evaluar constantemente el valor del negocio con respecto al pronóstico para verificar que el presupuesto ha sido correctamente utilizado.	

Tabla 46: Resumen de resultados PO5

Fuente: Creado por el autor

PO6: Comunicar las aspiraciones y la dirección de la gerencia	Grado de Madurez 3
FACTOR DE RIESGO: La gerencia no ha elaborado, documentado y comunicado un ambiente completo de administración de calidad y control de la información. El proceso de elaboración de políticas no es estructurado, mantenido y conocido por el personal, y las políticas, procedimientos y estándares existentes no son sólidos. La gerencia no ha reconocido totalmente la importancia de la conciencia de seguridad de TI y no ha iniciado programas de concienciación formales. El entrenamiento formal no está disponible para apoyar al ambiente de control de información, y no se aplica de forma rigurosa. Aunque existe un marco general de desarrollo para las políticas y estándares de control, el monitoreo del cumplimiento de estas políticas y estándares es inconsistente. Las técnicas para fomentar la conciencia de la seguridad no están estandarizadas y formalizadas.	
RECOMENDACIONES COBIT: ➢ Elaborar e implantar Políticas para TI, difundiendo a todo el personal de la empresa, para que tengan en cuenta que deben hacer para apoyar a los mismos y sepan a donde quieren llegar. ➢ Monitorear el cumplimiento de las mismas para que no queden solo en papeles.	

Tabla 47: Resumen de resultados PO6

Fuente: Creado por el autor

PO7: Administrar recursos humanos de TI	Grado de Madurez 3
FACTOR DE RIESGO: No hay un proceso definido y documentado para administrar los recursos humanos de TI. No hay un plan de administración de recursos humanos. No hay un enfoque estratégico para la contratación y la administración del personal de TI. No está establecido un programa de rotación, diseñado para expandir las habilidades gerenciales y de negocio.	
RECOMENDACIONES COBIT: ➢ Administrar los recursos humanos de TI y elaborar planes de contratación y entrenamiento adecuados. ➢ Evitar la sobre-dependencia de recursos clave para evitar problemas en caso de que los mismos no estén en algún momento ➢ Verificar con roles y responsabilidades si el personal es necesario y suficiente para las tareas del Departamento.	

Tabla 48: Resumen de resultados PO7

Fuente: Creado por el autor

PO9: Evaluar y administrar riesgos de TI	Grado de Madurez 2
FACTOR DE RIESGO: Existe un enfoque de evaluación de riesgos inmaduro y en evolución. La administración de riesgos se da por lo general a altos niveles y se aplica de manera típica solo a proyectos grandes o como respuesta a problemas. Los procesos de mitigación de riesgos están en implementación.	
RECOMENDACIONES COBIT: ➢ Elaborar de forma específica un Plan de Seguridad teniendo en cuenta todas las áreas de la empresa tanto interna como externamente. ➢ Aplicar los planes de seguridad de forma consciente ➢ Realizar permanentes evaluaciones de riesgo ➢ Recomendar y comunicar planes de acción para mitigar riesgos a todo el personal de la empresa.	

Tabla 49: Resumen de resultados PO9

Fuente: Creado por el autor

PO10: Administrar proyectos	Grado de Madurez 2
FACTOR DE RIESGO: Los proyectos de TI definen objetivos técnicos y de negocio de manera informal. Hay participación limitada de los interesados en la administración de los proyectos de TI. Las directrices iniciales se elaboran para muchos aspectos de la administración de proyectos pero no para todos. La aplicación a proyectos de las directrices administrativas se deja a discreción del gerente de proyecto.	
RECOMENDACIONES COBIT: ➢ Definir e implantar marcos y enfoques de programas y de proyectos ➢ Emitir directrices administrativas para proyectos ➢ Hacer la planeación para todos los proyectos incluidos en el portafolio de proyectos.	

Tabla 50: Resumen de resultados PO10

Fuente: Creado por el autor

AI1: Identificar soluciones automatizadas	Grado de Madurez 3
FACTOR DE RIESGO: No hay enfoques claros y estructurados para determinar las soluciones de TI. El enfoque para la determinación de las soluciones de TI requiere la consideración de alternativas evaluadas contra los requerimientos del negocio o del usuario, las oportunidades tecnológicas, la factibilidad económica, las evaluaciones de riesgo y otros factores. El proceso para determinar las soluciones de TI se aplica para algunos proyectos con base en factores tales como las decisiones tomadas por el personal involucrado, la cantidad de tiempo administrativo dedicado, y el tamaño y prioridad del requerimiento de negocio original. No se usan enfoques estructurados para definir requerimientos e identificar soluciones de TI.	
RECOMENDACIONES COBIT: ➢ Definir requerimientos técnicos y de negocio ➢ Realizar estudios de factibilidad económica, oportunidades tecnológicas para escoger la mejor solución. ➢ Aprobar (o rechazar) los requerimientos y los resultados de los estudios de factibilidad.	

Tabla 51: Resumen de resultados AI1

Fuente: Creado por el autor

AI2: Adquirir y mantener el software aplicativo	Grado de Madurez 3
FACTOR DE RIESGO: No hay un proceso claro, definido y de comprensión general para la adquisición y mantenimiento de software aplicativo. Se intenta aplicar los procesos de manera consistente a través de diferentes aplicaciones y proyectos. Las metodologías son por lo general, inflexibles y difíciles de aplicar en todos los casos, por lo que es muy probable que se salten pasos.	
RECOMENDACIONES COBIT: ➢ Elaborar un plan de adquisición y mantenimiento de Software que garantice tomar la mejor decisión. ➢ Definir estándares de desarrollo para todas las modificaciones ➢ Separar actividades de desarrollo, de pruebas y operativas	

Tabla 52: Resumen de resultados AI2

Fuente: Creado por el autor

AI3: Adquirir y mantener la infraestructura tecnológica	Grado de Madurez 3
FACTOR DE RIESGO: No hay un claro, definido y entendido proceso para adquirir y dar mantenimiento a la infraestructura TI. El proceso existente no respalda las necesidades de las aplicaciones críticas del negocio y no concuerda con la estrategia de negocio de TI. No se planea, programa y coordina el mantenimiento.	
RECOMENDACIONES COBIT: ➢ Establecer un plan de adquisición de tecnología que se alinee con el plan de infraestructura tecnológica ➢ Implantar medidas de control interno, seguridad y auditabilidad.	

Tabla 53: Resumen de resultados AI3

Fuente: Creado por el autor

AI4: Facilitar la operación y el uso	Grado de Madurez 3
FACTOR DE RIESGO: No hay un esquema bien definido, aceptado y comprendido para documentación del usuario, manuales de operación y materiales de entrenamiento. No se guarda y mantiene los procedimientos en una biblioteca formal y cualquiera que necesite saber no tiene acceso a ella. Las correcciones a la documentación y a los procedimientos se realizan por reacción. No hay un proceso que especifica las actualizaciones de procedimientos y los materiales de entrenamiento para que sea un entregable explícito de un proyecto de cambio. A pesar de la existencia de enfoques definidos, el contenido actual varía debido a que no hay un control para reforzar el cumplimiento de estándares. Los usuarios se involucran en los procesos informalmente. No se planea y programa tanto el entrenamiento del negocio como de los usuarios.	
RECOMENDACIONES COBIT: ➢ Implantar una política de documentación de tareas a todos los empleados del departamento para transferir el conocimiento y de esta manera apoyar al control y evaluación. ➢ Comunicar y entrenar a usuarios, a la gerencia del negocio, personal de apoyo y personal de operación	

Tabla 54: Resumen de resultados AI4

Fuente: Creado por el autor

AI5: Adquirir recursos de TI	Grado de Madurez 1
FACTOR DE RIESGO: La organización no ha reconocido la necesidad de tener políticas y procedimientos documentados que enlacen la adquisición de TI con el proceso general de adquisiciones de la organización. Los contratos para la adquisición de recursos de TI son elaborados y administrados por gerentes de proyecto u otras personas que ejercen su juicio profesional más que seguir resultados de procedimientos y políticas formales. Sólo existe una relación *ad hoc* entre los procesos de administración de adquisiciones y contratos corporativos de TI.	
RECOMENDACIONES COBIT: ➢ Asesorarse profesional, legal y contractualmente para adquirir algún recurso de TI. ➢ Definir procedimientos y estándares de adquisición ➢ Adquirir software y servicios requeridos de acuerdo con los procedimientos definidos	

Tabla 55: Resumen de resultados AI5

Fuente: Creado por el autor

AI6: Administrar cambios	Grado de Madurez 1
FACTOR DE RIESGO: No se reconoce que los cambios se deben administrar y controlar. Las prácticas varían y es muy probable que se puedan dar cambios sin autorización. Hay documentación de cambio pobre o no existente y la documentación de configuración es incompleta y no confiable. Es posible que ocurran errores junto con interrupciones al ambiente de producción, provocados por una pobre administración de cambios.	
RECOMENDACIONES COBIT: ➢ Evaluación, asignar prioridad y autorizar cambios ➢ Seguir el procedimiento y reporte de cambios	

Tabla 56: Resumen de resultados AI6

Fuente: Creado por el autor

AI7: Instalar y acreditar soluciones y cambios	Grado de Madurez 3
FACTOR DE RIESGO: No se cuenta con una metodología formal en relación con la instalación, migración, conversión y aceptación. Los procesos de TI para instalación y acreditación no están integrados dentro del ciclo de vida del sistema y no están automatizados. El entrenamiento, pruebas, transición y acreditación a producción tienen variaciones respecto al proceso definido, con base en las decisiones individuales.	
RECOMENDACIONES COBIT: ➢ Establecer una metodología de prueba a los cambios realizados. ➢ Evaluar y aprobar los resultados de las pruebas por parte de la gerencia del negocio ➢ Ejecutar revisiones posteriores a la implantación	

Tabla 57: Resumen de resultados AI7

Fuente: Creado por el autor

DS2: Administrar los servicios de terceros	Grado de Madurez 3
FACTOR DE RIESGO: No hay procedimientos bien documentados para controlar los servicios de terceros con procesos claros para tratar y negociar con los proveedores. Cuando se hace un acuerdo de prestación de servicios, la relación con el tercero no es meramente contractual. La naturaleza de los servicios a prestar no se detalla en el contrato y no incluye requerimientos legales, operacionales y de control. No se asigna la responsabilidad a algún miembro del departamento de supervisar los servicios de terceros. Los términos contractuales no se basan en formatos estandarizados. El riesgo del negocio asociado con los servicios del tercero no está valorado y esta reportado.	
RECOMENDACIONES COBIT: ➢ Establecer un procedimiento de contratación de servicios por terceros que garantice que estos cumplan a cabalidad con su trabajo y para tener un mejor control del uso de recursos.	

Tabla 58: Resumen de resultados DS2

Fuente: Creado por el autor

DS3: Administrar el desempeño y la capacidad	Grado de Madurez 2
FACTOR DE RIESGO: Los responsables del negocio y la gerencia de TI no están conscientes del impacto de no administrar el desempeño y la capacidad. Las necesidades de desempeño se logran por lo general con base en evaluaciones de sistemas individuales, el conocimiento y soporte de equipos de proyecto. Algunas herramientas individuales pueden utilizarse para diagnosticar problemas de desempeño y de capacidad, pero la consistencia de los resultados depende de la experiencia de individuos clave. No hay una evaluación general de la capacidad de desempeño de TI. Los problemas de disponibilidad son susceptibles de ocurrir de manera inesperada y aleatoria y toma mucho tiempo diagnosticarlos y corregirlos. Cualquier medición de desempeño se basa primordialmente en las necesidades de TI y no en las necesidades del cliente.	
RECOMENDACIONES COBIT: ➢ Administrar el desempeño capacidad y disponibilidad de los sistemas de la empresa.	

Tabla 59: Resumen de resultados DS3

Fuente: Creado por el autor

DS4: Garantizar la continuidad del servicio	Grado de Madurez 2
FACTOR DE RIESGO: No se asigna la responsabilidad a alguno de los miembros del departamento para mantener la continuidad del servicio. Los enfoques para asegurar la continuidad están fragmentados. Los reportes sobre la disponibilidad son esporádicos, pueden estar incompletos y no toman en cuenta el impacto en el negocio. No hay un plan de continuidad de TI documentado, aunque hay compromiso para mantener disponible la continuidad del servicio y sus principios más importantes se conocen. Existe un inventario de sistemas y componentes críticos, pero puede no ser confiable.	
RECOMENDACIONES COBIT: ➢ Desarrollar y mantener planes de contingencia de TI ➢ Difundir los planes de contingencia con entrenamiento y pruebas de los mismos. ➢ Guardar copias de los planes de contingencia y de los datos fuera de las instalaciones.	

Tabla 60: Resumen de resultados DS4

Fuente: Creado por el autor

DS5: Garantizar la seguridad de los sistemas	Grado de Madurez 2
FACTOR DE RIESGO: Las responsabilidades y la rendición de cuentas sobre la seguridad, no están asignadas a un coordinador de seguridad de TI. La conciencia sobre la necesidad de la seguridad esta fraccionada y limitada. Aunque los sistemas producen información relevante respecto a la seguridad, ésta no se analiza. Los servicios de terceros no cumplen con los requerimientos específicos de seguridad. Las políticas de seguridad se están desarrollando, pero las herramientas y las habilidades son inadecuadas. Los reportes de la seguridad de TI son incompletos. La capacitación sobre seguridad está disponible pero depende principalmente de la iniciativa del individuo. La seguridad de TI es vista primordialmente como responsabilidad y disciplina de TI, y el negocio no ve la seguridad de TI como parte de su propia disciplina.	
RECOMENDACIONES COBIT: ➢ Entender los requerimientos, vulnerabilidades y amenazas de seguridad. ➢ Administrar autorizaciones a los usuarios de forma estandarizada. ➢ Probar la seguridad de forma regular.	

Tabla 61: Resumen de resultados DS5

Fuente: Creado por el autor

DS7: Educar y entrenar a los usuarios	Grado de Madurez 2
FACTOR DE RIESGO: El programa de entrenamiento y educación, y los procesos asociados a lo largo de toda la organización está comenzando a identificarse en los planes de desempeño individuales de los empleados. Los procesos se desarrollan hasta la fase en la cual se imparte entrenamiento informal por parte de diferentes instructores. Sin embargo, hay comunicación consistente sobre los problemas globales y sobre la necesidad de atenderlos.	
RECOMENDACIONES COBIT: ➢ Establecer un plan de entrenamiento a usuarios ➢ Monitorear y reportar la efectividad del entrenamiento.	

Tabla 62: Resumen de resultados DS7

Fuente: Creado por el autor

DS8: Administrar la mesa de servicio y los incidentes	Grado de Madurez 2
FACTOR DE RIESGO: No hay conciencia organizacional de la necesidad de una función de mesa de servicio y de un proceso de administración de incidentes. Existe ayuda disponible de manera informal a través de una red de individuos expertos. Estos individuos tienen a su disposición algunas herramientas comunes para ayudar en la resolución de incidentes. No hay entrenamiento formal y la comunicación sobre procedimientos estándar y la responsabilidad es delegada al usuario.	
RECOMENDACIONES COBIT: ➢ Crear el servicio de una mesa de servicios ➢ Monitorear y reportar tendencias	

Tabla 63: Resumen de resultados DS8

Fuente: Creado por el autor

DS9: Administrar la configuración	Grado de Madurez 2
FACTOR DE RIESGO: La gerencia no esta consciente de la necesidad de controlar la configuración de TI y no entiende los beneficios de mantener información completa y precisa sobre las configuraciones. Las herramientas para la administración de configuraciones se utilizan hasta cierto grado, pero difieren entre plataformas. Además no se definen prácticas estandarizadas de trabajo. El contenido de la información de la configuración es limitado y no utilizan procesos interrelacionados, tales como administración de cambios y administración de problemas.	
RECOMENDACIONES COBIT: ➢ Establecer un repositorio central de todos los elementos de la configuración ➢ Identificar los elementos de configuración y su mantenimiento ➢ Revisar la integridad de los datos de configuración.	

Tabla 64: Resumen de resultados DS9

Fuente: Creado por el autor

DS10: Administración de problemas	Grado de Madurez 3
FACTOR DE RIESGO: No se acepta la necesidad de un sistema integrado de administración de problemas y no se evidencia con el apoyo de la gerencia y la asignación de presupuesto para personal y capacitación. El registro y rastreo de problemas y soluciones se dividen dentro del equipo de respuesta, utilizando las herramientas disponibles. Es poco probable detectar las desviaciones de los estándares y de las normas establecidas. La información no se comparte entre el personal de manera formal y proactiva. La revisión de incidentes y los análisis de identificación y resolución de problemas son limitados e informales.	
RECOMENDACIONES COBIT: ➢ Administrar y analizar causas raíz de los problemas reportados ➢ Tomar propiedad de los problemas y una resolución de problemas progresiva.	

Tabla 65: Resumen de resultados DS10

Fuente: Creado por el autor

DS11: Administración de datos	Grado de Madurez 2
FACTOR DE RIESGO: No hay conciencia sobre la necesidad de una adecuada administración de los datos. No se observa la propiedad y responsabilidad sobre los datos. Los requerimientos de seguridad para la administración de datos no son documentados por individuos clave. No se lleva a cabo algún tipo de monitoreo dentro de TI sobre algunas actividades clave de la administración de datos (respaldos, recuperación y desecho). Las responsabilidades para la administración de datos son asignadas de manera informal a personal clave de TI.	
RECOMENDACIONES COBIT: ➢ Realizar un plan de Respaldos más específico que el que ya se tiene, administrando el almacenamiento de datos en sitio y fuera de sitio ➢ Probar la restauración de la información ➢ Desechar de manera segura los datos y el equipo para que no puedan tener acceso personas que pueden hacer mal uso de la información.	

Tabla 66: Resumen de resultados DS11

Fuente: Creado por el autor

DS12: Administración del ambiente físico	Grado de Madurez 3
FACTOR DE RIESGO: Los controles ambientales, el mantenimiento preventivo y la seguridad física no cuentan con presupuesto autorizado y rastreado por la gerencia. No se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado. Los visitantes se registran a la entrada de la organización. Las instalaciones físicas mantienen un perfil bajo y son reconocibles de manera fácil. Las autoridades civiles no monitorean al cumplimiento con los reglamentos de salud y seguridad. Los riesgos se aseguran con el mínimo esfuerzo para optimizar los costos del seguro.	
RECOMENDACIONES COBIT: ➢ Implementar medidas de seguridad física. ➢ Administrar las instalaciones físicas de manera que se garantice la seguridad de los activos.	

Tabla 67: Resumen de resultados DS12

Fuente: Creado por el autor

DS13: Administración de operaciones	Grado de Madurez 2
FACTOR DE RIESGO: La organización no está consciente del rol clave que las actividades de operaciones de TI juegan en brindar funciones de soporte de TI. No se asignan presupuestos para herramientas con un criterio de caso por caso. Las operaciones de soporte de TI son informales e intuitivas. Hay una alta dependencia sobre las habilidades de los individuos. Las instrucciones de qué hacer, cuándo y en qué orden no están documentadas.	
RECOMENDACIONES COBIT: ➢ Administrar las operaciones del ambiente de TI en línea con los niveles de servicio acordados y con las instrucciones definidas.	

Tabla 68: Resumen de resultados DS13

Fuente: Creado por el autor

ME1: Monitorear y evaluar el desempeño de TI	Grado de Madurez 3
FACTOR DE RIESGO: La gerencia no ha comunicado e institucionalizado un proceso estándar de monitoreo. No se implantan programas educacionales y de entrenamiento para el monitoreo. Las evaluaciones todavía se realizan al nivel de procesos y proyectos individuales de TI y no están integradas a través de todos los procesos. No se definen herramientas para monitorear los procesos y los niveles de servicio de TI. Las mediciones de la contribución de la función de servicios de información al desempeño de la organización se definen, usando criterios financieros y operativos tradicionales. Las mediciones del desempeño específicas de TI, las mediciones no financieras, las estratégicas, las de satisfacción del cliente y los niveles de servicio no están definidas. No se ha definido un marco de trabajo para medir el desempeño.	
RECOMENDACIONES COBIT: ➢ Establecer programas de reportes de desempeño de proceso a reportes gerenciales ➢ Comparar el desempeño contra las metas acordadas e iniciar las medidas correctivas necesarias	

Tabla 69: Resumen de resultados ME1

Fuente: Creado por el autor

ME2: Monitorear y evaluar el control interno	Grado de Madurez 2
FACTOR DE RIESGO: La organización no utiliza reportes de control para comenzar iniciativas de acción correctiva. La evaluación del control interno depende de las habilidades de individuos clave. La organización no tiene mayor conciencia sobre el monitoreo de los controles internos. Se están empezando a usar metodologías y herramientas para monitorear los controles internos, aunque no se basan en un plan. Los factores de riesgo específicos del ambiente de TI se identifican con base en las habilidades de individuos.	
RECOMENDACIONES COBIT: ➢ Definir un sistema de controles interno integrado en el marco de trabajo de los procesos de TI ➢ Monitorear y reportar la efectividad de los controles internos sobre TI ➢ Reportar las excepciones de control a la gerencia para tomar acciones	

Tabla 70: Resumen de resultados ME2

Fuente: Creado por el autor

ME3: Garantizar el cumplimiento regulatorio	Grado de Madurez 3
FACTOR DE RIESGO: No se desarrollan, documentado y comunicado políticas, procedimientos y procesos, para garantizar el cumplimiento de los reglamentos y de las obligaciones contractuales legales. Se realiza poco monitoreo y existen requisitos de cumplimiento que no están resueltos. No se brinda entrenamiento sobre requisitos legales y regulatorios externos que afectan a la organización y no se instruye respecto a los procesos de cumplimiento definidos.	
RECOMENDACIONES COBIT: ➢ Establecer políticas y procedimientos para cumplir con requisitos legales y regulatorios relacionados con la TI	

Tabla 71: Resumen de resultados ME3

Fuente: Creado por el autor

4.2. Impacto de los criterios de información en el Departamento de Informática de Agua de los Andes S.A.

A continuación se presenta el informe del impacto de los criterios de información en AGUA DE LOS ANDES S.A. (Tabla 72 a Tabla 78).

CRITERIO DE INFORMACIÓN Efectividad	**Porcentaje** 60%
RECOMENDACIÓN COBIT: Para que exista una alta efectividad y llegue al 100% se recomienda que la información importante y referente a los procesos del negocio sea oportuna, correcta, consistente y utilizable.	

Tabla 72: Resumen de resultados criterio: Efectividad

Fuente: Creado por el autor

CRITERIO DE INFORMACIÓN Eficiencia	**Porcentaje** 47,09%
RECOMENDACIÓN COBIT: Para que exista una alta eficiencia y llegue al 100% se recomienda que la información que se obtenga sea optimizando los recursos de TI.	

Tabla 73: Resumen de resultados criterio: Eficiencia

Fuente: Creado por el autor

CRITERIO DE INFORMACIÓN Confidencialidad	**Porcentaje** 12,09%
RECOMENDACIÓN COBIT: Para que exista una alta confidencialidad y llegue al 100% se recomienda que la información sensible contra divulgación no autorizada se le otorgue una debida protección contra intrusos o extraños al departamento.	

Tabla 74: Resumen de resultados criterio: Confidencialidad

Fuente: Creado por el autor

CRITERIO DE INFORMACIÓN Integridad	**Porcentaje** 12,08%
RECOMENDACIÓN COBIT: Para que exista una alta integridad y llegue al 100% se recomienda que la información entregada al mismo mantenga su validez de acuerdo con los valores y expectativas del negocio, así como también exista precisión y suficiencia de la información.	

Tabla 75: Resumen de resultados criterio: Integridad

Fuente: Creado por el autor

CRITERIO DE INFORMACIÓN Disponibilidad	**Porcentaje** 4,77%
RECOMENDACIÓN COBIT: Para que exista una alta disponibilidad y llegue al 100% se recomienda que la información cuando es requerida por el proceso del negocio ahora y en el futuro se encuentre disponible, así como también se debe tomar en cuenta la protección de los recursos de TI y las capacidades asociadas.	

Tabla 76: Resumen de resultados criterio: Disponibilidad

Fuente: Creado por el autor

CRITERIO DE INFORMACIÓN Cumplimiento	**Porcentaje** 9,05%
RECOMENDACIÓN COBIT: Para que exista un alto cumplimiento y llegue al 100% se recomienda que se lleve un adecuado cumplimiento de las leyes, regulaciones, y acuerdos contractuales a los que el proceso del negocio está sujeto.	

Tabla 77: Resumen de resultados criterio: Cumplimiento

Fuente: Creado por el autor

CRITERIO DE INFORMACIÓN Confiabilidad	**Porcentaje** 8,90%
RECOMENDACIÓN COBIT: Para que exista una alta confiabilidad y llegue al 100% se recomienda que se entregue una información adecuada para que la gerencia administre la entidad y ejerza sus responsabilidades de reportes financieros y de cumplimiento.	

Tabla 78: Resumen de resultados criterio: Confiabilidad

Fuente: Creado por el autor

Como promedio total del impacto de los criterios de información se obtuvo el valor de 22,01%, lo que en comparación con el 100% es bajo en su impacto.

5.- Presentación del Informe Final

5.1. Informe Ejecutivo

El presente informe muestra los resultados de la evaluación de los procesos que establece COBIT, practicada al Departamento de Informática, en base a los grados de madurez.

A continuación (Tabla 79) se presentan un resumen de los resultados obtenidos, con los cuales la empresa y la dirección de TI pueden darse

cuenta en el nivel que están ubicados para analizar y poner en práctica las recomendaciones enunciadas en la anterior sección.

PO1: Definir el plan estratégico de TI	Grado de Madurez 3
PO2: Definir la arquitectura de la información	Grado de Madurez 2
PO3: Determinar la dirección tecnológica	Grado de Madurez 3
PO4: Definir procesos, organización y relaciones de TI	Grado de Madurez 3
PO5: Administrar la inversión en TI	Grado de Madurez 1
PO6: Comunicar las aspiraciones y la dirección de la gerencia	Grado de Madurez 3
PO7: Administrar recursos humanos de TI	Grado de Madurez 3
PO9: Evaluar y administrar riesgos de TI	Grado de Madurez 2
PO10: Administrar proyectos	Grado de Madurez 2
AI1: Identificar soluciones automatizadas	Grado de Madurez 3
AI2: Adquirir y mantener el software aplicativo	Grado de Madurez 3
AI3: Adquirir y mantener la infraestructura tecnológica	Grado de Madurez 3
AI4: Facilitar la operación y el uso	Grado de Madurez 3
AI5: Adquirir recursos de TI	Grado de Madurez 1
AI6: Administrar cambios	Grado de Madurez 1
AI7: Instalar y acreditar soluciones y cambios	Grado de Madurez 3
DS2: Administrar los servicios de terceros	Grado de Madurez 3
DS3: Administrar el desempeño y la capacidad	Grado de Madurez 2
DS4: Garantizar la continuidad del servicio	Grado de Madurez 2
DS5: Garantizar la seguridad de los sistemas	Grado de Madurez 2
DS7: Educar y entrenar a los usuarios	Grado de Madurez 2
DS8: Administrar la mesa de servicio y los incidentes	Grado de Madurez 2
DS9: Administrar la configuración	Grado de Madurez 2

DS10: Administración de problemas	Grado de Madurez 3
DS11: Administración de datos	Grado de Madurez 2
DS12: Administración del ambiente físico	Grado de Madurez 3
DS13: Administración de operaciones	Grado de Madurez 2
ME1: Monitorear y evaluar el desempeño de TI	Grado de Madurez 3
ME2: Monitorear y evaluar el control interno	Grado de Madurez 2
ME3: Garantizar el cumplimiento regulatorio	Grado de Madurez 3

Tabla 79: Grados de madurez en los que se encuentra el Departamento de Informática

Fuente: Creado por el autor

A continuación (Tabla 80) se presenta los grados de madurez tomados como referencia:

0	No existe	No se aplican procesos administrativos en lo absoluto.
1	Inicial	Los procesos son iníciales y desorganizados.
2	Repetible	Los procesos siguen un patrón regular.
3	Definido	Los procesos se documentan y se comunican.
4	Administrado	Los procesos se monitorean y se miden.
5	Optimizado	Las buenas prácticas se siguen y se automatizan.

Tabla 80: Referencia del valor del modelo de madurez

Fuente: Creado por el autor

El cálculo de porcentaje de los criterios de información se presenta a continuación

(Tabla 81):

Efectividad	**60,00 %**
Eficiencia	**47.09 %**
Confidencialidad	**12.09 %**
Integridad	**12.08 %**
Disponibilidad	**4.77 %**
Cumplimiento	**9.05 %**
Confiabilidad	**8.90 %**
Promedio de los criterios de información	**22.01 %**

Tabla 81: Resumen de Resultados

Fuente: Creado por el autor

A continuación se presenta gráficamente (Figura 5) el porcentaje obtenido por cada uno de los criterios de la información, para tener una visión más clara del estado que se encuentra el departamento:

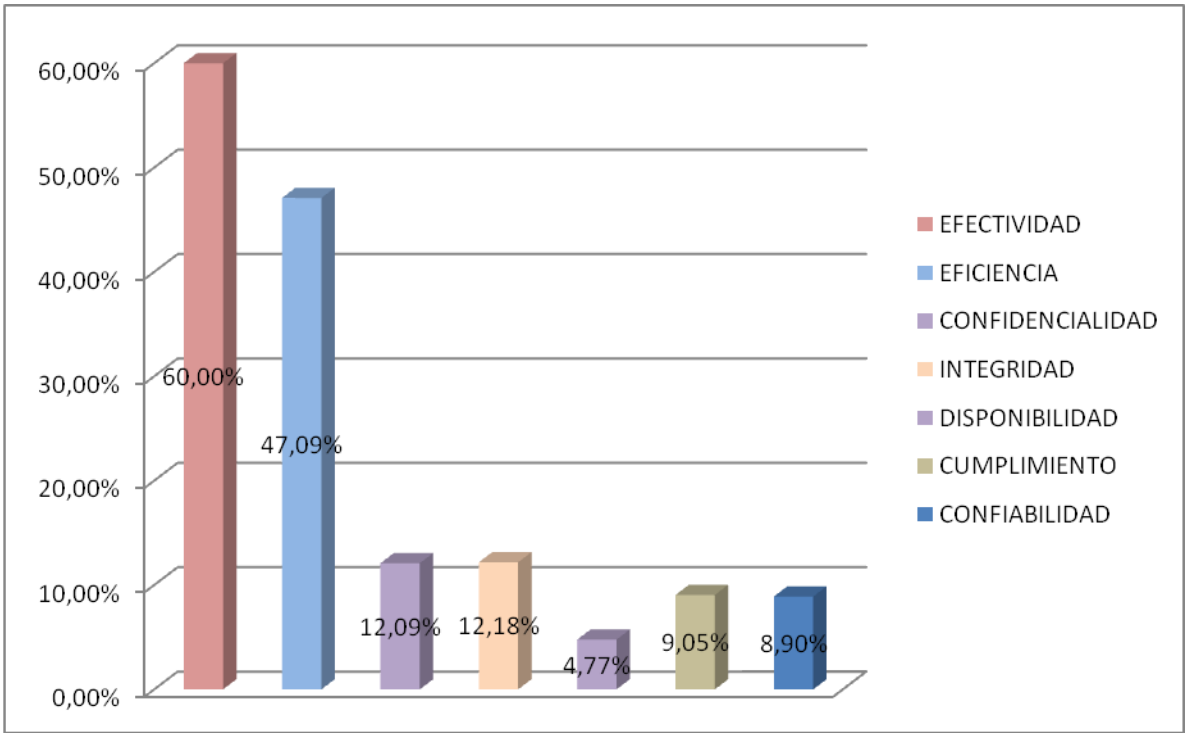

Figura 5: Impacto de los criterios de información en el Departamento de Informática

Fuente: Realizado por el autor

El Promedio general obtenido de los criterios de la información es del 21,01%.

6.- Conclusiones y Recomendaciones

6.1. Conclusiones

- Los objetivos de control planteados por COBIT se relacionan de manera directa con el ambiente de manejo y evaluación de riesgos, los mismos que pueden ser entendidos tanto por la Gerencia como por el Departamento de Informática.

- El Jefe del Departamento de Informática de Agua de los Andes S.A. puede asegurar que proporciona un sistema de control de riesgos adecuado para el ambiente de TI si administra adecuadamente los Objetivos de Control de alto nivel que se encuentran distribuidos en los Dominios de COBIT.

- Los Modelos de Madurez de COBIT para el control sobre los procesos de TI dan un punto claro de donde la organización está actualmente y son un punto de partida para fijar una meta futura de ascenso hasta llegar al nivel óptimo.

- La utilización de una norma internacional como lo es la ISO 17799 para el manejo de la seguridad dentro de un área de TI ayudó a conocer la situación

actual de la organización para luego seleccionar los objetivos de control de COBIT indicados para evaluarlos.

- Se encontró procesos con grado de madurez 1, lo que quiere decir que estos son iníciales y desorganizados.

- Se determinó el impacto de los procesos de TI sobre la efectividad (60%), eficiencia (47,09%), confidencialidad (12,09%), integridad (12,08%), disponibilidad (4,77%), cumplimiento (9,05%) y confiabilidad (8,90%), dando un promedio de 22,01%; lo que nos indica que la organización se encuentra en un nivel bajo en cuanto a gestión de riesgos de TI.

6.2. Recomendaciones

- Se recomienda documentar todos los procesos de TI en forma gráfica y escrita, para establecer controles de seguridad de la información y de esta manera evitar que la misma sea vulnerable ante errores y fallas.

  Además, Agua de los Andes S.A., debe tener un Plan Estratégico actualizado que sirva como guía y ayuda, y este pueda elaborar su propio Plan Estratégico conjuntamente ligado al general.

- Tomar en cuenta los factores de riesgos y recomendaciones dadas, ya que va a ser de gran aporte para mejorar el desempeño y así orientar su trabajo y esfuerzo al desarrollo de toda la organización.

- Se recomienda que inicie un proceso de implementación de un modelo de control que puede ser COBIT, ya que esta metodología es fruto de un compendio de experiencias y recomendaciones de profesionales a nivel mundial.

- La Gerencia de TI del departamento debe tomar en consideración los procesos que se encuentran en un grado de madurez 1; ya que los mismos están en un estado crítico y requieren atención inmediata.

- Tomar en consideración los porcentajes obtenidos acerca de los criterios de información que tiene que ver con efectividad, eficiencia, confiabilidad, integridad, disponibilidad, confidencialidad y cumplimiento, para que de esta manera poder cubrir las debilidades que tenga y lograr así un mejor desempeño.

Referencias Bibliográficas

1.- COMER, Douglas E.(1996), Redes globales de información con internet y TCP/IP. Editorial Prentice Hall. Tercera Edición. México.

2.- ECHENIQUE GARCIA (2001), José Antonio. Auditoría en Informática. Editorial McGraw-Hill. Segunda Edición. México.

3.- PIATTINI VELTHIUS,(2001) Mario Gerardo, PESO NAVARRO, Emilio del. Auditoría Informática: Un enfoque práctico. Editorial Ra-MA, Segunda Edición, Madrid.

4.- SLOSSE, Carlos A. (1990), Auditoría: Un Nuevo Enfoque Empresarial, Editorial Macchi. Segunda Edición. Buenos Aires.

5.- STALLINGS, William (1997), Comunicaciones y redes de computadoras. Editorial Prentice Hall. Quinta edición. Madrid.

6.- TANENBAUM, Andrew S. (1997), Redes de computadoras. Editorial Prentice Hall. Tercera Edición. México.

7.- Documentación facilitada por Agua de los Andes S.A.

Medios Electrónicos

1. Agua de los Andes S.A.(2009). Recuperado el 12 de Enero de 2011, de http://www.adlandes.com.ar/

2. El Sistema de Gestión de Seguridad de la Información (2004). Códigos de Buenas Prácticas de Seguridad. Recuperado el 23 de Noviembre de 2011, de http://www.shutdown.es/ISO17799.pdf.

3. Estándar ISO/IEC.I nternacional. 17799 Segunda Edición (2005). Recuperado el 23 de Noviembre de 2011 de https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

4. IT Governance Institute (2007). Cobit 4.1.Recuperado el 22 de Mayo de 2011, de http://cs.uns.edu.ar/~ece/auditoría/cobiT4.1spanish.pdf

5. Wikipedia (2012). Recuperado el 02 de Febrero de 2012, de http://es.wikipedia.org/wiki/Objetivos_de_control_para_la_informaci%C3%B3n_y_tecnolog%C3%ADas_relacionadas

Anexo 1

Relevamiento

HARDWARE EXISTE EN LA EMPRESA

Características de los servidores

Existen dos servidores con las siguientes características:

Servidor 1 HP

- Marca: HP Proliant SL 170z G6
- Software: Windows Server 2008.
- Memoria: 6 GB (3 X 2 GB) de memoria estándar.
- Disco: Seis discos duros de 250 Gb.
- Procesador: Intel

Servidor 2 AS/400

- Marca: IBM System I 520 Modelo 9406-520
- Software: Windows Server 2008.
- Memoria: 32 Gb.

- Disco: 39 Tb.
- Procesador: Performance 600-7100 CPW

Características de las PC'S

La empresa en su totalidad posee alrededor de 200 PC´s, de las cuales 100 están en la casa central.

El 60% de estas PC´s es de marca Hewlett Packard y el resto clones.

En sus principios no contaban con aplicaciones gráficas, sino con el sistema AS/400. Al ir migrando a aplicaciones y sistemas operativos gráficos, fueron adquiriendo clones con mayor capacidad, actualizando el motherboard, el procesador, el gabinete y la cantidad de memoria RAM, y conservando el resto del hardware.

La empresa ha tomado la decisión de asegurar su red, debido al gran costo que implicaba contratar un mantenimiento tercerizado permanentemente.

PLAN ESTRATÉGICO

El Departamento de Informática no tiene un Plan estratégico específico[10], en cuanto al Plan Informático, este plan existe pero se lo tiene en borrador,

[10] Informado por el Jefe del Departamento de Informática

se lo utiliza más como una agenda de actividades que se propone realizar a corto y largo plazo.

En cuanto a programas de capacitación, no se tiene un Plan de Capacitación establecido, se lo realiza cuando se requiera y en forma informal. Si se trata de una capacitación interna, ésta es impartida por el propio personal dependiendo del área de conocimiento. Para el caso en que se presentan proyectos que requieran de conocimientos con los que no cuenta el personal de la Unidad Informática, se realiza una capacitación externa bajo pedido de los usuarios.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

CONTROL DE ACCESO A EQUIPOS

Todas las máquinas de la empresa disponen de disqueteras, puertos USB y grabadoras de DVD, aunque el 90% de los usuarios no las necesita. Solo algunas máquinas de administración que reciben archivos de otras entidades deben utilizarlas como medios de entrada de datos, a pesar de que se está empezando a utilizar Internet para el intercambio de información.

Estos dispositivos están habilitados y no hay ningún control sobre ellos, no se hacen controles automáticos de virus ni se prohíbe el booteo desde estos dispositivos. Nunca hubo robo de datos usando medios externos, solo fue necesario hacer bloqueos de las impresoras para restringir los datos de salida del sistema, previniendo posibles fraudes.

Los gabinetes donde se ubican los switches de cada una de las sucursales, están cerrados con llave, para evitar que el personal de limpieza o cualquier persona desconecten las entradas, y como medida de precaución, debido a que hay bocas libres en estos dispositivos. Las llaves de todos los gabinetes están en el Departamento de Informática de casa central, en poder del administrador del sistema. Todos ellos están ubicados fuera del alcance del personal (a la altura del techo, o en espacios donde hay poca circulación de personal).

No se realizan controles periódicos sobre los dispositivos de hardware instalados en las PC´s, de manera que alguien podría sacar o poner alguno. Una vez que se ha completado la instalación de algún equipo, el administrador del sistema no realiza chequeos rutinarios o periódicos, solo revisa los equipos ante fallas en los por un problema reportado por el usuario.

Los servidores no se apagan en horarios no laborales, permanecen en funcionamiento las 24 horas del día.

POLÍTICA DE SEGURIDAD

Política de seguridad de la información

El departamento Informática no cuenta con un plan de acción para afrontar riesgos de seguridad, ni con reglas para el mantenimiento de cierto nivel de seguridad.[11]

[11] Informado por el Jefe del Departamento de Informática

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Organización interna

No existe compromiso por parte de la gerencia para apoyar activamente la seguridad dentro de la organización. La gerencia no invierte en seguridad informática y no lo ve como un aspecto importante.

No se asignan responsabilidades. Cuando la seguridad es atacada, generalmente las personas dentro de la organización tratan de buscar un culpable y quedar libres de todo cargo. La asignación de responsabilidades es verbal.

Grupos o personas externas

En el momento de la instalación no se efectuó un análisis de costo-beneficio para determinar que controles serían necesarios implementar.

Existe un circuito cerrado de cámaras de video. Este sistema no es exclusivo del departamento, ya que las cámaras están en toda el área administrativa de la empresa, ubicadas en puntos estratégicos, como en la puerta de ingreso, pero ninguna de éstas cámaras apuntan al departamento o a su puerta de ingreso.

La empresa cuenta con una Empresa tercerizada de seguridad, en horarios laborales se ubican en el interior y exterior de la misma, y cuando se cierra la empresa solo quedan en el exterior, porque queda activado el sistema de alarma.

El personal de la empresa que tiene el acceso permitido al departamento es el de cómputos y gerentes.

Además del personal antes mencionado, tienen autorización personal de empresas tercerizadas como el de limpieza y seguridad.

GESTIÓN DE ACTIVOS

Responsabilidades sobre los activos

Se tiene asignado responsabilidades por cada uno de los activos de la organización, poseen un inventario de todos los activos que se tienen, a quien /quienes les pertenecen, el uso que se les debe dar, y la clasificación de todos los activos pero no está realizado con ningún tipo de formato especificado por normas de manejo de seguridad.

No se tiene documentado ni implementadas reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información.

Clasificación de la información

La información de la empresa no es clasificada. La información debe ser clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información.

SEGURIDAD DE RECURSOS HUMANOS

Antes del empleo

Si es necesario y si la gerencia aprueba, el jefe del Departamento Informática solicita personal a Recursos Humanos detallando las características que debe reunir. De acuerdo a entrevista al Jefe cada vez que se contrato una nueva persona no reunía las características solicitadas.

Durante el desempeño de funciones

Si bien se definen claramente los roles y responsabilidades de cada empleado, todo es acuerdo verbal. En la práctica todos realizan distintas actividades de acuerdo a las necesidades y conocimientos.

También se deben especificar las responsabilidades cuando se da el cese del empleo o cambio de puesto de trabajo, para que la persona no se vaya simplemente y deje a la organización afectada de alguna manera en materia de seguridad.

SEGURIDAD FÍSICA Y AMBIENTAL

Estructura del edificio

Cuando se construyó el edificio de la empresa, no se tuvo en cuenta el diseño del Departamento de Informática y sus condiciones de seguridad. Por este motivo se construyo posteriormente en el fondo del edificio, para restringir el

acceso. Está ubicado en el primer piso, mientras que en la planta baja se ubica la atención al público y el resto de los Departamentos.

Las paredes externas son elevadas y las ventanas tienen rejas soldadas y vidrios espejados que impiden la visibilidad desde el exterior del mismo.

El equipamiento informático fue provisto por una empresa que se encargó del asesoramiento técnico. A estos proveedores les consultaron cuáles eran los requisitos mínimos necesarios para que las garantías cubriesen los equipamientos (la instalación eléctrica necesaria, la refrigeración correcta del área, los métodos de aislamiento magnético, entre otros.) Para determinar qué medidas tomar en la instalación se realizó un análisis costo – beneficio. El nuevo sector se diseño pensando en su futuro crecimiento y actualmente sus instalaciones se encuentran convenientemente ubicadas, con la posibilidad de expandirse sin inconvenientes.

Equipos de seguridad

Dispone de los siguientes dispositivos de Seguridad:

Aire acondicionado y calefacción: la temperatura se mantiene en 19ºC. Cuentan con dos equipos de refrigeración central, y en el departamento de Informática hay dos equipos adicionales de aire acondicionado, solo para esta área, con el fin de mantener esta temperatura en verano. Estas especificaciones las sugirió el personal que provee los equipamientos.

Matafuegos: Son equipos químicos, manuales y están instalados y mantenidos por el Departamento de Seguridad e Higiene, quienes deciden el lugar de ubicación, el departamento de Informática cuenta con dos propios, uno ubicado dentro del Departamento y el otro ubicado en la habitación de los servidores.

Alarmas contra intrusos: existe una alarma en la empresa que se activa en los horarios no comerciales, generalmente de noche cuando se cierra la empresa.

Generador de energía: En la empresa cuentan con un generador de energía Marca Deutz de 30Kva, 24 Kw que alimenta exclusivamente al departamento informática. Existe una central automática (Tablero de Transferencia) ubicada en un pasillo interno fuera del departamento de informática que funciona tanto en modo manual o automática; esta central detecta un fallo en la red de suministro eléctrico, obligando el arranque inmediato del Grupo Electrógeno. El departamento cuenta con conexión trifásica propia, dicha conexión ingresa al Tablero de transferencia, de allí salen dos cables, uno que va al generador ubicado en el techo y el otro que alimenta al departamento.

UPS: (Uninterruptible Power Supply) Posee dos UPS en serie que pueden mantener los servidores y las máquinas de desarrollo funcionando.

Características de los UPS:

Marca: UPS TRV Pro 500 VA net.

Año de instalación: 2010.

Estabilizador incorporado.

Cuatro salidas 220 V.

Potencia 500 / 700 VA.

Batería interna.

Autonomía: 15 minutos.

Protección contra descarga total de batería.

Protección contra sobrecarga y cortocircuito.

Filtro de línea.

Estos UPS están instalados de forma tal que trabajan en conjunto con el generador de energía.

Estabilizador de tensión: La Empresa cuenta con tres líneas de corriente eléctrica, una línea es exclusiva para los servidores.

Descarga a tierra: Existe una jabalina que funciona como descarga a tierra para el edificio.

Luz de emergencia: Existe una luz de emergencia que permanece en carga las 24 horas del día y en el caso de un corte de luz se activa automáticamente. Se verifico con personal del departamento de Seguridad e Higiene que su funcionamiento es correcto.

Archivo General: Existe un archivo general de la empresa ubicado en otro edificio. El edificio cuenta con un sector específico para el área informática donde se almacenan todo lo enviado por ese sector en estantes dentro de cajas metálicas etiquetadas con fecha. No se lleva un control de lo archivado.

GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES, CONTROL DE ACCESO Y ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

USUARIOS DEL SISTEMA

ALTA DE USUARIO: Cuando la empresa contrata a una nueva persona el Jefe del Departamento al que va a pertenecer solicita por nota al Jefe del departamento el alta de un nuevo usuario de acceso a red y usuario del sistema. Si bien se solicita por nota, no existe un formato de nota ni se documenta en ningún lugar las solicitudes recibidas.

En el Departamento informática se crea un nuevo usuario con los permisos básicos de ese departamento.

Características usuario de sistema:

ID: Consta de seis dígitos, los tres primeros dígitos corresponden al Departamento donde trabaja y los tres últimos el próximo número disponible (ej.: CAT014, Departamento Catastro usuario N° 14).

Clave: Inicialmente será el mismo que el usuario y se solicita al usuario para que la modifique.

Grupo al que pertenece: Departamento Catastro y Medición.

Fecha de expiración: La clave expira a los 30 días, el sistema automáticamente a los 25 días envía un mensaje cada vez que se ingresa al sistema informando que la clave está por expirar. Pasados los 30 días sin modificar la clave el usuario se bloquea.

Contador de intentos fallidos: Si el usuario ha ingresado mal la contraseña tres veces seguidas se bloquea, en este caso el jefe de departamento debe solicitar por nota al jefe de informática la reactivación de la cuenta.

CARACTERÍSTICAS USUARIO DE ACCESO A RED:

ID: Consta de ocho dígitos, los dos primeros dígitos corresponden al nombre de la empresa, los próximos tres dígitos corresponden al Departamento donde trabaja y los tres últimos el próximo número disponible (ej.: AACAT014, Empresa Agua de los andes, Departamento Catastro usuario N° 14).

Clave: Es el mismo que el usuario, el sistema no solicita modificación ni es posible hacerlo ya que no existe un botón para realizar tal modificación.

Fecha de expiración: La clave nunca expira.

Contador de intentos fallidos: No existe un contador de intentos fallidos, si el usuario ha ingresado mal la contraseña automáticamente se borra el campo donde se ingresa la clave. No muestra ninguna ventana indicando que se ingreso mal la clave y se puede ingresar todas las veces que uno desee claves incorrectas sin que el usuario se bloquee.

Baja de usuario

Cuando un usuario deja de pertenecer al departamento no hay ningún procedimiento para dar de baja a ese usuario, por lo general al pasar los 30 días sin uso se bloquea automáticamente. Se detecto en muchos casos que personal que pasa a otro sector cuenta con dos usuarios de sistema.

Control de modificaciones

No se lleva a cabo ninguna revisión ni control sobre los permisos que tienen asignados.

Inactividad con el sistema

Si el usuario permanece un período de 5 minutos sin actividad, el sistema se cierra automáticamente.

Cuentas de usuario

Los usuarios del sistema pueden tener abiertos, al mismo tiempo, todos los menús a los que están autorizados, y varias sesiones del mismo menú. No se hacen restricciones en cuanto a la cantidad de sesiones que los usuarios pueden utilizar simultáneamente.

El administrador puede logearse desde cualquier terminal de la empresa lo que resulta riesgoso ya que podría, por error, abandonar ese puesto de trabajo dejando esa terminal logeada con su usuario administrador.

Autenticación

En la pantalla de login de los sistemas se muestran los siguientes datos:

- Nombre de usuario (a completar por el usuario).
- Clave (a completar por el usuario)
- Opción para cambiar el password.
- Salir

Una vez que algún usuario ha logrado logearse en el sistema, aparece en pantalla arriba a la izquierda el nombre del usuario logeado.

Los datos de autenticación de los usuarios del sistema de la empresa se almacenan en el servidor de aplicaciones, en un archivo de texto plano, sin ningún control de acceso.

Dentro de la empresa no se usa ningún tipo de firma digital, ni para mensajes internos ni para los externos ya que las directivas de importancia no son enviadas vía mail.

En cuanto a la configuración de las estaciones de trabajo, no hay ningún control de acceso a sus sistemas BIOS[12], de manera que al momento del encendido de la máquina cualquier persona podría modificar sus opciones de configuración.

[12] Basic Input / Output System

Permisos

Los nuevos usuarios cuentan con una serie de permisos básicos. La asignación o denegación de nuevos permisos a los usuarios los solicita el jefe de Departamento a través de un requerimiento.

El sistema informático está desglosado en una gran cantidad de módulos diferentes, donde cada uno de ellos es un programa en sí mismo. De esta manera cada usuario del sistema, dispone de los accesos directos a los programas que corresponden a su área. Así, los usuarios solo pueden interactuar con los datos a los que dichos módulos les permiten acceder.

Generación de Passwords

Los Passwords que existen en la empresa son generados en forma manual, sin procedimientos automáticos de generación. Como restricción, deben tener una longitud máxima de 10 caracteres, numéricos o alfanuméricos.

Cuando se da de alta un empleado en el sistema, su password se inicializa con el mismo nombre de la cuenta, advirtiéndole al usuario que lo cambie, pero sin realizar ningún control sobre la modificación del mismo.

Cambios de passwords

Los cambios en los passwords los hacen los usuarios a través de la pantalla del login, allí hay un botón que muestra la opción para su modificación.

Si un usuario olvida su password, debe advertirle al administrador del sistema mediante requerimiento, aprobado el requerimiento el administrador modifica la clave dejando el mismo nombre de usuario y contraseña (EJ.: USUARIO: CAT004 CONTRASEÑA: CAT004).

Al informar de esta modificación, no se requiere que el usuario modifique la contraseña, no se controla esta situación. Ocurre lo mismo cuando un usuario ingresa mal su contraseña tres veces seguidas: el sistema lo bloqueará y el usuario no podrá ingresar, por lo que deberá recurrir al administrador.

SEGURIDAD DE REDES Y ACCESO A INTERNET

Topología de red

La topología de red utilizada en la empresa consiste en nodos colocados en forma de árbol. Dicha conexión en árbol es parecida a una serie de redes en estrella interconectadas.

Es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones.

Componentes de red

La red informática de la empresa se compone del siguiente equipamiento:

- Doscientas PC´s distribuidas en toda la empresa, con aproximadamente cien de ellas en la Casa Central.
- Dos Servidores, Hewlett Packard e IBM AS/400.
- Un enlace de fibra óptica.
- Cableado interno UTP categoría 5.
- Conexión de internet ADSL de 1 KBPS.
- Tres Patcheras Marca AMP de 24 Bocas.
- Siete Switch 10/100 de 24 puertos, Marca: 3Com, Modelo: Baseline Switch 2024.
- Un RAS, Marca: 3Com, Modelo: SuperStack II 1500 Base Unit

CONEXIÓN INTERNA Y EXTERNA

Conexión interna: La totalidad del tendido de cables en el interior de la Casa Central se realizó con UTP categoría 5.

Conexión externa: Existe una conexión a través de fibra óptica que conecta la Casa Central con el resto de las sucursales, dicha conexión y mantenimiento se encuentra tercerizada por la Empresa NoaNet (http://www.noanet.com.ar).

RESPALDO O BACK-UP

Cuenta con una política de respaldos.

Backup de datos en el servidor

Cuando se realiza un cambio en la configuración del servidor, se guardan copias de las configuraciones anterior y posterior al cambio, pero no se documentan los cambios que se realizan ni la fecha de estas modificaciones.

No hay ningún procedimiento formal para la realización ni la recuperación de los backups. Además no se realizan chequeos para comprobar que el funcionamiento sea el correcto.

Los backups se deberían hacer los martes y jueves a las 15 hs. y los sábados a primera hora de la mañana según indicaciones del Jefe pero no se cumplen. Es un proceso que no está automatizado, cada desarrollador copia los archivos que ha modificado durante el día a una carpeta del servidor de aplicaciones (\\Srvalvear\Sistemas\Imputacion Preventiva). Luego se agregan los archivos de la empresa modificados por los usuarios. Una vez generada esta carpeta, el administrador del sistema la zipea y copia este archivo a DVD regrabables que se almacenan en el mismo departamento.

Estos backups son incrementales, es decir que se agregan a la carpeta los archivos modificados, debido a esto es imposible recuperar versiones antiguas de aplicaciones desarrolladas y luego modificadas, ya que se sobrescriben con

las versiones nuevas. No se hacen backups de cada una de las versiones del sistema por separado, se resguardan los datos a medida que van siendo modificados.

Backup de datos en las pc´s

Los usuarios deben realizar sus propios backups de los datos almacenados en sus máquinas, ya que estos datos son propiedad de los empleados. Generalmente no se realizan, debido a que los archivos que almacenen son de soporte o de poca importancia para la empresa.

Los usuarios han sido instruidos a almacenar en la carpeta Mis Documentos todos los datos que ellos generen. Si hacen un backup deberían hacerlo en sus propias máquinas o en el servidor

Backup de la página web

El encargado de la pagina Web un backup de la página web completa en una PC del departamento, pero sin una frecuencia preestablecida.

Protección de los backups

Los empleados no dieron mucha información al respecto solamente que están protegidos con contraseñas.

Documentación del backup

No existe documentación escrita sobre los datos del backup dónde se hace esta copia ni datos históricos referidos a la restauración de los mismos.

SEGURIDAD DE RED

Configuración de servicios del firewall

El Firewall de Windows Server 2008 es un firewall con estado basado en host que permite o bloquea el tráfico de red según su configuración y las aplicaciones que se encuentran en ejecución, para proteger la red de usuarios y programas malintencionados.

El Firewall permitir interceptar tanto el tráfico entrante como el saliente. El administrador de red puede, por ejemplo, configurar el nuevo Firewall de Windows con un conjunto de excepciones para bloquear todo el tráfico que se envía a puertos específicos, como puertos conocidos usados por software de virus o especificar direcciones que contengan contenido confidencial o no deseable. Esto protege al equipo de virus que podrían propagarse a través de la red y protegen a la red de virus que pueden intentar propagarse desde un sistema en riesgo.

Se pudo observar que el administrador realiza verificaciones pero no se documentan.

Protección de acceso a redes

La protección de acceso a redes (NAP) evita que equipos que no se encuentran en buen estado tengan acceso a la red de la organización y la pongan en peligro. NAP se usa para configurar y aplicar requisitos de estado de cliente,

y para actualizar, o corregir, equipos cliente con incumplimiento antes que se puedan conectar a la red corporativa.

Con NAP el administrador puede configura directivas de estado que definen por ejemplo requisitos de software, requisitos de actualización de seguridad y opciones de configuración necesarias en equipos que se conectan a la red de la organización.

Se pudo observar que el administrador realiza verificaciones pero no se documentan.

Servicio de Internet

Para la conexión a Internet se utiliza un servidor de una Empresa tercerizada E.J.E.S.A. La conexión se configuró utilizando WINDOWS SERVER 2008 y el programa LogMeIn de forma que solo tienen conexión al exterior un rango de direcciones IP definido por la Gerencia.

Dentro de los IP con servicio existe una restricción en el acceso de acuerdo a la jerarquía y necesidades en la empresa, en la mayoría de los casos se encuentran bloqueadas:

- Servicios de chat entre los más conocidos MSN, Skype y Messenger Yahoo.
- Redes sociales como Faceboock y Twitter.
- Páginas pornográficas, de música, de videos y de juegos.

- Páginas de descarga como RapidShare, Mediafire, entre otras.
- Páginas de correo electrónico como Hotmail, Gmail y Yahoo Mail.
- Buscadores como Google y Yahoo.

Otros Sitios Webs no seguros para la empresa no especificados por el administrador.

Servicio de mail

El sistema de mail está alojado en el servidor de Internet de la empresa tercerizada E.J.E.S.A. El mail tiene como dominio @adlandes.com.ar.

El correo se lee con Outlook Express en las PC´s de la empresa.

No todos los empleados tienen una cuenta de mail ya que hay muchos que no necesitan este servicio.

Si un empleado necesita una dirección de mail, porque su puesto de trabajo lo amerita, el Jefe del área al que pertenece realiza un requerimiento al administrador de Informática, y éste le asigna una casilla de correo.

Los empleados no usan el mail solamente para funciones laborales, sino también con fines personales. No se realizan controles, de manera que pueden usarlo para cualquier fin. No se hace ningún control para comprobar si los usuarios se suscriben a listas de correo, no hay prohibiciones en este sentido.

Incidente en la Seguridad de la Información

El Departamento no tiene una política de reporte de debilidades, sino que según sea el caso de emergencia se soluciona dichas eventualidades pero no con un procedimiento determinado, no se ha informado a los usuarios que se tome nota y se reporte cualquier debilidad de seguridad observada o sospechada en el sistema o los servicios.

No se tiene un registro de eventualidades que han sido solucionadas, para su monitoreo y procurar que no vuelvan a suceder.

Gestión de la Continuidad del Negocio

No existe un plan de contingencia donde se tome en cuenta aspectos de la seguridad de la información de la gestión de la continuidad del negocio.

Únicamente para salvaguardar la información se realizan respaldos.

Cumplimiento de los requerimientos legales

No todo el software cuenta con las licencias de uso respectivas y en regla.

No se cuenta con una política apropiada con respecto al uso de licencias y que garantice los derechos de propiedad intelectual de los sistemas que se han implementado así como con una política de protección y privacidad de los datos.

CUMPLIMIENTO DE LAS POLÍTICAS Y ESTÁNDARES DE SEGURIDAD, Y CUMPLIMIENTO TÉCNICO

La seguridad de los sistemas de información se revisa cada vez que es requerido, es decir, cuando se detecta algún error debido a la falta de seguridad.

El Jefe de Departamento verifica el cumplimiento de los procedimientos de seguridad dentro del área y en caso de un incumplimiento se pide rendición de cuentas.

La detección de vulnerabilidades en los sistemas lo hacen las personas del departamento y también los usuarios finales.

AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

No se ha realizado auditoría de los sistemas de información, ni internamente ni externamente.

Anexo 2

Estándar Internacional ISO/IEC

ISO es el acrónimo de International Organization for Standardization. Aunque si se observan las iniciales para el acrónimo, el nombre debería ser IOS, los fundadores decidieron que fuera ISO, derivado del griego "*isos",* que significa "igual". Por lo tanto, en cualquier país o en cualquier idioma, el nombre de la institución es ISO, y no cambia de acuerdo a la traducción de "International Organization for Standardization" que corresponda a cada idioma. Se trata de la organización desarrolladora y publicadora de Estándares Internacionales más grande en el mundo. ISO es una red de instituciones de estándares nacionales de 157 países, donde hay un miembro por país, con una Secretaría Central en Geneva, Suiza, que es la que coordina el sistema.

ISO es una organización no gubernamental que forma un puente entre los sectores públicos y privados.

Respecto al origen de la organización ISO, oficialmente comenzó sus operaciones el 23 de febrero de 1947 en Geneva, Suiza. Nació con el objetivo de "facilitar la coordinación internacional y la unificación de los estándares industriales."

IEC es el acrónimo de International Electrotechnical Commission. Esta es una organización sin fines de lucro y también no gubernamental. Se ocupa de preparar y publicar estándares internacionales para todas las tecnologías eléctricas o relacionadas a la electrónica.

IEC nace en 1906 en London, Reino Unido, y desde entonces ha estado proporcionando estándares globales a las industrias electrotécnicas mundiales. Aunque como se acaba de decir, IEC nació en el Reino Unido, en el año de 1948 movieron su sede a Geneva, Suiza, ciudad en la que también se encuentra la sede de ISO.

ISO e IEC han establecido un comité técnico conjunto denominado ISO/IEC JTC1 (ISO/IEC Joint Technical Committee). Este comité trata con todos los asuntos de tecnología de la información. La mayoría del trabajo de ISO/IEC JTC1 es hecho por subcomités que tratan con un campo o área en particular. Específicamente el subcomité SC 27 es el que se encarga de las técnicas de seguridad de las tecnologías de información. Dicho subcomité ha venido desarrollando una familia de Estándares Internacionales para el Sistema Gestión y Seguridad de la Información. La familia incluye Estándares Internacionales sobre requerimientos, gestión de riesgos, métrica y medición, y el lineamiento de implementación del sistema de gestión de seguridad de la información

La información puede existir en muchas formas, por ejemplo puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por

correo o utilizando medios electrónicos o hablada en una conversación. Sea cual sea la forma en la que se tenga la información, debe estar en todo caso protegida.

La seguridad de la información se logra implementando un conjunto adecuado de controles, políticas, procesos, procedimientos, estructuras organizacionales, y otras acciones que hagan que la información pueda ser accedida sólo por aquellas personas que están debidamente autorizadas para hacerlo.

Es importante y necesario para las empresas realizar una evaluación de riesgos para identificar amenazas para los activos, así como también para conocer y analizar la vulnerabilidad y la probabilidad de ocurrencia de accesos, robo o alteración de la información, y el impacto potencial que esto llegaría a tener. Una vez se hayan identificado los riesgos, se procede a seleccionar controles apropiados a implementar para asegurar que los riesgos se reduzcan a un nivel aceptable.

Vulnerabilidad

Es una debilidad o agujero en la seguridad de la información, que se puede dar por causas como las siguientes, entre muchas otras:

- Falta de mantenimiento
- Personal sin los conocimientos adecuados o necesarios
- Desactualización de los sistemas críticos

Amenaza

Es una declaración intencionada de hacer un daño, como por ejemplo mediante un virus, un acceso no autorizado o robo. Pero no se debe pensar que únicamente personas pueden ser los causantes de estos daños, pues existen otros factores como los eventos naturales, que son capaces de desencadenar daños materiales o pérdidas inmateriales en los activos, y son también consideradas como amenazas.

Ataque

Es una acción intencional e injustificada (desde el punto de vista del atacado). Consiste en un intento por romper la seguridad de un sistema o de un componente del sistema.

Riesgo

Es una potencial explotación de una vulnerabilidad de un activo de información por una amenaza. Se valora como una función del impacto, amenaza, vulnerabilidad y de la probabilidad de un ataque exitoso.

Atacante

Es alguien que deliberadamente intenta hacer que un sistema de seguridad falle, encontrando y explotando una vulnerabilidad.

Los atacantes pueden ser internos (que pertenecen a la organización) o externos (que no pertenecen a la organización). Respecto a los atacantes internos, son difíciles de detener porque la organización está en muchas maneras forzada a confiar en ellos. Estos conocen cómo trabaja el sistema y cuáles son sus debilidades. Quizás el error más común de seguridad es gastar considerables recursos combatiendo a los atacantes externos, ignorando las amenazas internas.

Estándar Internacional ISO/IEC 17799

Luego de haber definido algunos conceptos y conocimientos preliminares y de hablar de manera general sobre la organización ISO y el comité IEC, es momento de entrar en detalle y profundizar específicamente en el tema concerniente a esta investigación: el Estándar Internacional ISO/IEC 17799.

El documento del Estándar Internacional ISO/IEC 17799, después de la introducción, se divide en quince capítulos. En este documento se presentará un resumen y análisis de cada uno de los quince capítulos, de manera breve.

Alcance

Este Estándar Internacional va orientado a la seguridad de la información en las empresas u organizaciones, de modo que las probabilidades de ser afectados por robo, daño o pérdida de información se minimicen al máximo.

Estructura de este Estándar

Este Estándar contiene un número de categorías de seguridad principales, entre las cuales se tienen once cláusulas:

a) Política de seguridad.
b) Aspectos organizativos de la seguridad de la información.
c) Gestión de activos.
d) Seguridad ligada a los recursos humanos.
e) Seguridad física y ambiental.

f) Gestión de comunicaciones y operaciones.

g) Control de acceso.

h) Adquisición, desarrollo y mantenimiento de los sistemas de información.

i) Gestión de incidentes en la seguridad de la información.

j) Gestión de la continuidad del negocio.

k) Cumplimiento.

Evaluación de los riesgos de seguridad

Se deben identificar, cuantificar y priorizar los riesgos de seguridad. Posterior a ello se debe dar un tratamiento a cada uno de los riesgos, aplicando medidas adecuadas de control para reducir la probabilidad de que ocurran consecuencias negativas al no tener una buena seguridad.

La reducción de riesgos no puede ser un proceso arbitrario y regido por la voluntad de los dueños o administradores de la empresa, sino que además de seguir medidas adecuadas y eficientes, se deben tener en cuenta los requerimientos y restricciones de la legislación y las regulaciones nacionales e internacionales, objetivos organizacionales, bienestar de clientes y trabajadores, costos de implementación y operación (pues existen medidas de seguridad de gran calidad pero excesivamente caras, tanto que es más cara la seguridad que la propia ganancia de una empresa, afectando la rentabilidad).

Se debe saber que ningún conjunto de controles puede lograr la seguridad completa, pero que sí es posible reducir al máximo los riesgos que amenacen con afectar la seguridad en una organización.

Política de seguridad

Su objetivo es proporcionar a la gerencia la dirección y soporte para la seguridad de la información, en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes. Esto por supuesto debe ser creado de forma particular por cada organización. Se debe redactar un *"Documento de la política de seguridad de la información."* Este documento debe ser primeramente aprobado por la gerencia y luego publicado y comunicado a todos los empleados y las partes externas relevantes.

El *Documento de la Política de Seguridad de la Información* debe contar con un claro lineamiento de implementación, y debe contener partes tales como una definición de seguridad de la información, sus objetivos y alcances generales, importancia, intención de la gerencia en cuanto al tema de seguridad de la información, estructuras de evaluación y gestión de riesgos, explicación de las políticas o principios de la organización, definición de las responsabilidades individuales en cuanto a la seguridad. Se debe tener especial cuidado respecto a la confidencialidad de este documento, pues si se distribuye fuera de la organización, no debería divulgar información confidencial que afecte de alguna manera a la organización o a personas

específicas (por ejemplo que afecte la intimidad de alguien al divulgar sus datos personales)

Las políticas de seguridad de la información no pueden quedar estáticas para siempre, sino que por el contrario, tienen que ser continuamente revisadas y actualizadas para que se mantengan en condiciones favorables y en concordancia con los cambios tecnológicos o cualquier tipo de cambio que se dé. Por ejemplo, si aparece un nuevo virus o nuevas tecnologías que representen riesgos, las políticas de seguridad podrían cambiar o ser mejoradas de acuerdo a las necesidades actuales. Un caso práctico sería el aparecimiento de las memorias USB. Antiguamente esa tecnología no existía, entonces no se esperaba que existieran robos de información a través de puertos USB. Ahora las memorias USB son de uso global y por lo tanto, las políticas de seguridad deberían considerar bloquear puertos USB o algo por el estilo, para no permitir que se extraiga información de esa manera de forma ilícita o por personas no autorizadas.

Otro problema sería tener excelentes políticas de seguridad, pero que no sean implementadas correctamente o que simplemente se queden a nivel teórico y que no se apliquen. En la vida real se suelen dar casos donde las leyes están muy bien redactadas, pero que no se cumplen. Sucede en muchos países, que la legislación puede estar estructurada muy bien, pero que no se respeta. Igualmente podría darse que se tengan excelentes políticas, pero que no se cumplan o que no se sepan implementar correctamente. Por lo tanto, se requieren lineamientos de implementación adecuados.

Aspectos organizativos de la seguridad de la información

La organización de la seguridad de la información se puede dar de dos formas: *organización interna* y *organización con respecto a terceros.*

En cuanto a la organización interna, se tiene como objetivo manejar la seguridad de la información dentro de la organización.

Se requiere un compromiso por parte de la gerencia para apoyar activamente la seguridad dentro de la organización. La gerencia debe invertir en seguridad, y no verlo como un aspecto que no tiene relevancia. Algunas veces la seguridad requiere inversión económica, y parte del compromiso de la gerencia implica tener un presupuesto especial para seguridad, por supuesto de una forma razonable que no afecte la rentabilidad de la empresa. Por ejemplo, implementar un método carísimo de seguridad podría ser de gran beneficio, pero representar un costo demasiado elevado.

Es fundamental también *asignar responsabilidades.* Es típica una tendencia humana el echarle la culpa a otros. Entonces cuando la seguridad es atacada, casi siempre las personas dentro de la organización tratan de buscar un culpable y quedar libres de todo cargo. Por esa razón se deben asignar claramente responsabilidades para que cuando se den los problemas, cada quien responda por sus actos y por lo que estaba bajo su cargo. La asignación de responsabilidades no

solamente tiene que ser verbal, sino que escrita y en muchas ocasiones, incluso bajo un contrato legal.

Deben también existir acuerdos de confidencialidad. También se debe tener en cuenta mantener los contactos apropiados con las autoridades relevantes, por ejemplo con la policía o con el departamento de bomberos. También se debe saber en qué casos se debe contactar a estas instituciones. También se deben mantener contactos apropiados con grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales, así como contar con capacitaciones en materia de seguridad.

La organización en materia de seguridad de la información debe también considerarse respecto a terceros. El objetivo de esto es mantener la seguridad de la información y los medios de procesamiento de información de la organización que son ingresados, procesados, comunicados a, o manejados por, grupos externos. Para ello se debe comenzar por la identificación de los riesgos relacionados con los grupos externos. Se debe estudiar cómo a raíz de procesos comerciales que involucran a grupos externos se les puede estar otorgando acceso que afecte la seguridad. Esto se puede dar tanto con clientes o con proveedores. Se debe tener especial cuidado respecto a los contratos que se hagan con terceros, para no afectar la seguridad de la información.

Gestión de activos

Se deben asignar responsabilidades por cada uno de los activos de la organización, así como poseer un inventario actualizado de todos los activos que se tienen, a quien/quienes les pertenecen, el uso que se les debe dar, y la clasificación de todos los activos. Para esto el departamento de contabilidad tendrá que hacer un buen trabajo en cuanto a esta clasificación y desglose de activos, y el departamento de leyes de la empresa también tendrá que ser muy metódico en estos procesos, ya que los activos son todos los bienes y recursos que posee una empresa, incluyendo bienes muebles e inmuebles, dinero, entre otras. Por lo tanto este es un asunto delicado y de gran importancia.

Seguridad ligada a los recursos humanos

El objetivo de esto es asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados, reduciendo el riesgo de robo, fraude y mal uso de los medios. Es necesario definir claramente los roles y responsabilidades de cada empleado. Todo esto no debe ser simplemente mediante acuerdos verbales, sino que se debe plasmar en el contrato de trabajo. También deben existir capacitaciones periódicas para concientizar y proporcionar formación y procesos disciplinarios relacionados a la seguridad y responsabilidad de los recursos humanos en este ámbito.

También se deben especificar las responsabilidades cuando se da el cese del empleo o cambio de puesto de trabajo, para que la persona no se vaya simplemente y deje a la organización afectada de alguna manera en materia de seguridad.

Seguridad física y ambiental

La seguridad física y ambiental se divide en *áreas seguras* y *seguridad de los equipos.* Respecto a las áreas seguras, se refiere a un perímetro de seguridad física que cuente con barreras o límites tales como paredes, rejas de entrada controladas por tarjetas o recepcionistas, y medidas de esa naturaleza para proteger las áreas que contienen información y medios de procesamiento de información.

Se debe también contar con controles físicos de entrada, tales como puertas con llave. Además de eso, es necesario considerar la seguridad física con respecto a amenazas externas y de origen ambiental, como incendios (para los cuales deben haber extintores adecuados y en los lugares convenientes), terremotos, huracanes, inundaciones y atentados terroristas. Deben también haber áreas de acceso público de carga y descarga, parqueos, áreas de visita, entre otros. Si hay gradas, deben ser seguras y con las medidas respectivas como antideslizantes y barras de apoyo sobre la pared para sujetarse.

En cuanto a la seguridad ambiental, se debe controlar la temperatura adecuada para los equipos, seguridad del cableado, mantenimiento de

equipos. Para todo esto se requerirá de los servicios de técnicos o ingenieros especializados en el cuidado y mantenimiento de cada uno de los equipos, así como en la inmediata reparación de los mismos cuando sea necesario. La ubicación de los equipos también debe ser adecuada y de tal manera que evite riesgos. Por ejemplo si algún equipo se debe estar trasladando con frecuencia, quizá sea mejor dejarlo en la primera planta, en vez de dejarlo en la última planta de un edificio, pues el traslado podría aumentar los riesgos de que se caiga y dañe, especialmente si no se cuenta con un ascensor. Se debe igualmente verificar y controlar el tiempo de vida útil de los equipos para que trabajen en condiciones óptimas.

Gestión de comunicaciones y operaciones

El objetivo de esto es asegurar la operación correcta y segura de los medios de procesamiento de la información.

En primer lugar, es necesario que los procedimientos de operación estén bien documentados, pues no basta con tener las ideas en la mente de los administradores, sino que se deben plasmar en documentos que por supuesto estén autorizados por la gerencia.

Otro aspecto fundamental es la gestión de cambios. Un cambio relevante no se debe hacer jamás sin documentarlo, además de la necesidad de hacerlo bajo la autorización pertinente y luego de un estudio y análisis de los beneficios que traerá dicho cambio.

Se debe tener cuidado que nadie pueda tener acceso, modificar o utilizar los activos sin autorización o detección. Para ello debe haber una bitácora de accesos, con las respectivas horas y tiempos de acceso.

Es completamente necesario tener un nivel de separación entre los ambientes de desarrollo, de prueba y de operación, para evitar problemas operacionales.

Si la organización se dedica a vender servicios, debe implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros.

A la hora de aceptar un nuevo sistema, se debe tener especial cuidado, verificando primeramente las capacidades y contando con evaluadores capacitados para determinar la calidad o falta de calidad de un sistema nuevo a implementar. Se tienen que establecer criterios de aceptación de los sistemas de información, actualizaciones o versiones nuevas, y se deben realizar pruebas adecuadas a los sistemas durante su desarrollo y antes de su aceptación.

La protección contra el código malicioso y descargable debe servir para proteger la integridad del software y la integración con los sistemas y tecnologías con que ya se cuenta. Se deben también tener controles de detección, prevención y recuperación para proteger contra códigos maliciosos, por ejemplo antivirus actualizados y respaldos de información. De hecho, los respaldos de información son vitales y deben realizarse con una frecuencia razonable, pues de lo contrario, pueden existir pérdidas de información de gran impacto negativo.

En cuanto a las redes, es necesario asegurar la protección de la información que se transmite y la protección de la infraestructura de soporte. Los servicios de red tienen que ser igualmente seguros, especialmente considerando cómo la tendencia de los últimos años se encamina cada vez más a basar todas las tecnologías de la información a ambientes en red para transmitir y compartir la información efectivamente. Los sistemas tienen que estar muy bien documentados, detalle a detalle, incluyendo por supuesto la arquitectura de red con la que se cuenta.

Se tienen que establecer políticas, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación. Además de las medidas directas para proteger el adecuado intercambio de información, se le debe recordar al personal el tomar las precauciones adecuadas, como no revelar información confidencial al realizar una llamada telefónica para evitar ser escuchado o interceptado por personas alrededor suyo, intervención de teléfonos, personas en el otro lado de la línea (en el lado del receptor). Igualmente para los mensajes electrónicos se deben tomar medidas adecuadas, para evitar así cualquier tipo de problema que afecte la seguridad de la información.

Cuando se haga uso del comercio electrónico, debe haber una eficiente protección cuando se pasa a través de redes públicas, para protegerse de la actividad fraudulenta, divulgación no autorizada, modificación, entro otros.

Debe haber un continuo monitoreo para detectar actividades de procesamiento de información no autorizadas. Las auditorías son también necesarias.

Las fallas deben ser inmediatamente corregidas, pero también registradas y analizadas para que sirvan en la toma de decisiones y para realizar acciones necesarias.

Los relojes de todos los sistemas de procesamiento de información relevantes dentro de una organización o dominio de seguridad deben estar sincronizados con una fuente que proporcione la hora exacta acordada. Asimismo, todo acceso a la información debe ser controlado.

Control de acceso

En primer lugar, se debe contar con una política de control de acceso. Todo acceso no autorizado debe ser evitado y se deben minimizar al máximo las probabilidades de que eso suceda. Todo esto se controla mediante registro de usuarios, gestión de privilegios, autenticación mediante usuarios y contraseñas.

Aparte de la autenticación correspondiente, los usuarios deben asegurar que el equipo desatendido tenga la protección apropiada, como por ejemplo la activación automática de un protector de pantalla después de cierto tiempo de inactividad, el cual permanezca impidiendo el acceso hasta que se introduzca una contraseña conocida por quien estaba autorizado para utilizar la máquina desatendida.

Son necesarios controles de acceso a la red, al sistema operativo, a las aplicaciones y a la información. Para todo esto deben existir registros y bitácoras de acceso.

Deben también existir políticas que contemplen adecuadamente aspectos de comunicación móvil, redes inalámbricas, control de acceso a ordenadores portátiles, y teletrabajo, en caso que los empleados de la empresa ejecuten su trabajo fuera de las instalaciones de la organización.

Adquisición, desarrollo y mantenimiento de los sistemas de información

Contemplar aspectos de seguridad es requerido al adquirir equipos y sistemas, o al desarrollarlos. No solamente se debe considerar la calidad y el precio, sino que la seguridad que ofrecen.

Debe existir una validación adecuada de los datos de entrada y de salida, controlando el procesamiento interno en las aplicaciones, y la integridad de los mensajes.

La gestión de claves debe ser tal que ofrezca soporte al uso de técnicas criptográficas en la organización, utilizando técnicas seguras.

Garantizar la seguridad de los archivos del sistema es fundamental, por lo que se debe controlar el acceso a los archivos del sistema y el código fuente del programa, y los proyectos de tecnologías de información y las actividades de soporte se deben realizar de manera segura.

Deben establecerse procedimientos para el control de la instalación del software en los sistemas operacionales. Con esto por ejemplo se evita el riesgo de realizar instalaciones ilegales o sin las respectivas licencias.

Se debe restringir el acceso al código fuente para evitar robos, alteraciones, o la aplicación de ingeniería inversa por parte de personas no autorizadas, o para evitar en general cualquier tipo de daño a la propiedad de código fuente con que se cuente.

La seguridad en los procesos de desarrollo y soporte debe considerar procedimientos de control de cambios, revisiones 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.

Contar con un control de las vulnerabilidades técnicas ayudará a tratar los riesgos de una mejor manera.

Gestión de incidentes en la seguridad de la información

La comunicación es fundamental en todo proceso. Por lo tanto, se debe trabajar con reportes de los eventos y debilidades de la seguridad de la información, asegurando una comunicación tal que permita que se realice una acción correctiva oportuna, llevando la información a través de los canales gerenciales apropiados lo más rápidamente posible. De la misma manera se debe contar con

reportes de las debilidades en la seguridad, requiriendo que todos los empleados, contratistas y terceros de los sistemas y servicios de información tomen nota de y reporten cualquier debilidad de seguridad observada o sospechada en el sistema o los servicios.

Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información es elemental.

Aprender de los errores es sabio. Por ello, se deben establecer mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información, siempre con la idea de no volver a cometer los errores que ya se cometieron, y mejor aún, aprender de los errores que ya otros cometieron.

A la hora de recolectar evidencia, cuando una acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (ya sea civil o criminal); se debe recolectar, mantener y presentar evidencia para cumplir con las reglas de evidencia establecidas en la(s) jurisdicción(es) relevante(s).

Gestión de la continuidad del negocio

Las consecuencias de los desastres, fallas en la seguridad, pérdida del servicio y la disponibilidad del servicio debieran estar sujetas a un análisis del impacto comercial. Se deben desarrollar e implementar planes para la continuidad

del negocio para asegurar la reanudación oportuna de las operaciones esenciales. La seguridad de la información debiera ser una parte integral del proceso general de continuidad del negocio, y otros procesos gerenciales dentro de la organización.

Se debe contar con planes de continuidad del negocio que incluyan la seguridad de la información. Estos planes no deben ser estáticos, sino que deben ser actualizados y ser sometidos a pruebas, mantenimiento y reevaluación.

Junto a la gestión de riesgos, debe aparecer la identificación de eventos que pueden causar interrupciones a los procesos, junto con la probabilidad y el impacto de dichas interrupciones y sus consecuencias para la seguridad de la información. Por supuesto se requieren planes alternativos y de acción ante tales eventos, asegurando siempre la protección e integridad de la información y tratando de poner el negocio en su estado de operación normal a la mayor brevedad posible.

Cumplimiento

Es una prioridad el buen cumplimiento de los requisitos legales para evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad. La identificación de la legislación aplicable debe estar bien definida.

Se deben definir explícitamente, documentar y actualizar todos los requerimientos legales para cada sistema de información y para la organización en general.

Es necesario implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso del material con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentado.

El cumplimiento de los requisitos legales se aplica también a la protección de los documentos de la organización, protección de datos y privacidad de la información personal, prevención del uso indebido de los recursos de tratamiento de la información, y a regulaciones de los controles criptográficos.

Los sistemas de información deben estar bajo monitoreo y deben chequearse regularmente para ver y garantizar el cumplimiento de los estándares de implementación de la seguridad.

En cuanto a las auditorías de los sistemas de información, se tiene que maximizar la efectividad de y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información. Durante las auditorías de los sistemas de información deben existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría. También se requiere protección para salvaguardar la integridad y evitar el mal uso de las herramientas de auditoría.

Las actividades y requerimientos de auditoría que involucran chequeos de los sistemas operacionales deben ser planeados y acordados cuidadosamente para minimizar el riesgo de interrupciones en los procesos.

Glosario

Activo: cualquier cosa que tenga valor para la organización.

Amenaza: una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización.

Análisis de riesgo: uso sistemático de la información para identificar las fuentes y calcular el riesgo.

Control: medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. El control también se utiliza como sinónimo de salvaguarda o contramedida.

Criptografía: es el arte o ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que sólo puedan ser leídos por las personas a quienes van dirigidos.

Electrotecnia: es la ciencia que estudia las aplicaciones técnicas de la electricidad.

Evaluación del riesgo: proceso de comparar el riesgo estimado con un criterio de riesgo dado para determinar la importancia del riesgo.

Evento de seguridad de la información: cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red, indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

Gestión del riesgo: actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

Incidente de seguridad de la información: un incidente de seguridad de la información es indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

Lineamiento: descripción que aclara qué se debiera hacer y cómo, para lograr los objetivos establecidos en las políticas.

Medios de procesamiento de la información: cualquier sistema, servicio o infraestructura de procesamiento de la información, o los locales físicos que los alojan.

Métrica: es una metodología de planificación, desarrollo y mantenimiento de sistemas de información.

Política: intención y dirección general expresada formalmente por la gerencia.

Riesgo: combinación de la probabilidad de un evento y su ocurrencia.

Seguridad de la información: preservación de confidencialidad, integración y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no-reputación y confiabilidad.

Tercera persona: persona u organismo que es reconocido como independiente de las partes involucradas, con relación al ítem en cuestión.

Tratamiento del riesgo: proceso de selección e implementación de medidas para modificar el riesgo.

Vulnerabilidad: la debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

Anexo 3

Cuestionarios

Para el desarrollo del trabajo fue necesario entrevistar a distintos usuarios del sistema y demás personas que interactúan con él. En el presente anexo se adjuntan los cuestionarios utilizados para la realización de éstas entrevistas.

TEMA: HARDWARE DE LA EMPRESA

Encuestados: Reparador de Pc y Encargado de Redes

Características del Servidor
• Tipo y marca de servidor.
• Capacidad de procesamiento.
• Cantidad de memoria.
• Capacidad de disco.
• Dispositivos varios.
• UPS o sistemas de alimentación alternativa del servidor.

Características de las PC´s.
• Cantidad.
• Características particulares.
• Características generales.

Backup
• Dispositivos de back up utilizados.

TEMA: SOFTWARE DE LA EMPRESA

Encuestados: Desarrolladores de Software y Jefe de Departamento.

Software
• Software del servidor.
• Software de las PC´s.
• Aplicaciones bases en cada sector de la empresa.
• Gestión de virus.
• Detalle de aplicaciones.
• Licencias.

Usuarios
• Responsabilidades en el Departamento de informática
o Responsables de Bases de datos
o Responsables de Aplicaciones
o Responsables de Servicio Técnico
• Tipo de perfiles de usuarios según sectores
o Clasificación del perfil
o Accesos del perfil a aplicaciones o datos.

TEMA: POLÍTICAS DE SEGURIDAD

Encuestados: Desarrolladores de Software y Jefe de Departamento.

Políticas de Seguridad
• ¿Existe algún plan estratégico con respecto a la Seguridad Lógica de la Empresa?
• ¿La Gerencia está al tanto de la Seguridad Informática?

• ¿Existen políticas de seguridad? ¿Están Documentadas?
• ¿La Empresa realiza inversiones para mejorar la Seguridad?
• ¿Existen controles internos?
• ¿Existe un plan de contingencia en caso de Problemas?

TEMA: ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Encuestados: Jefe de Departamento

IDENTIFICACIÓN – ID'S
Altas
• ¿Qué datos hay en el perfil del usuario cuando se hace un alta? ¿Se guardan los siguientes datos?
○ ID de usuario,
○ Nombre y apellido completo,
○ Puesto de trabajo y departamento de la empresa,
○ Jefe inmediato,
○ Descripción de tareas
• Consentimiento a que auditen sus actividades en el sistema, y de que conoce las normas de buen uso del sistema.
○ Explicaciones breves y claras de cómo elegir su clave.
○ Tipo de cuenta al que pertenece cada empleado.
○ Fecha de expiración de la cuenta.
○ Datos de los permisos de acceso y excepciones.
○ Restricciones horarias para el uso de recursos.
• ¿Que otros datos del usuario son necesarios en el ID? ¿Que datos guardan en la planilla de personal?

• ¿El ID de usuario puede repetirse?
• ¿Si una cuenta de usuario fue borrada o eliminada, puede utilizarse para un usuario nuevo?

Bajas
• ¿Cómo se relacionan con los de R.R.H.H.? ¿El departamento de R.R.H.H. se encarga de comunicar las modificaciones en el personal? ¿Qué se hace al respecto? ¿Cómo se actualiza la lista?
• ¿Cómo se administran los despidos (o desvinculación del personal)? ¿Se tiene en cuenta una política de despidos para evitar actos de vandalismo por posibles disgustos de los empleados desvinculados de la empresa?
• ¿Hay algún histórico de las cuentas que se dan de baja?
• ¿Se guardan los archivos y datos de las cuentas eliminadas? ¿Por cuánto tiempo? ¿Qué datos se guardan? ¿Con qué motivo?

Mantenimiento
• ¿Hay procedimientos para asignar los usuarios a un grupo de acuerdo al sector donde realiza su trabajo?
• ¿Hay procedimientos para dar de alta, baja, modificar, suspender. Una cuenta de usuario?
• ¿Se hacen revisiones de las cuentas de usuarios? ¿Se revisan sus permisos?
• ¿Hay procedimientos para determinar los nuevos requerimientos relacionados con cambios en funciones del empleado? ¿Cómo se mantienen actualizadas las cuentas cuando esto pasa?
• ¿Se documentan las modificaciones que se hacen en las cuentas? ¿Se lleva un histórico de los cambios?

Permisos
• ¿Tienen una clasificación de los recursos (datos) en base a la sensibilidad? ¿O en base a los tipos (base de datos, archivos de configuración, datos personales, según el departamento de la organización.?
• ¿Tienen distinción de los tipos de accesos que tiene cada usuario a cada recurso?
• ¿Quién les asigna los permisos a los usuarios?

ID Inactivas
• ¿Después de qué período de inactividad en que el usuario no realiza acciones en el sistema, se limpia la pantalla asociada al usuario, se desconecta el usuario inactivo o pide la clave nuevamente?
• Antes de terminar con la sesión, ¿se avisa al usuario que se lo desconectará?
• Si en un determinado tiempo el usuario no responde, ¿entonces se termina la sesión?
• ¿Después de qué período de inactividad (de cuantos días) se pone una cuenta de usuario como inactiva, porque el usuario no se ha logeado? ¿Este proceso es automático (del sistema operativo) o lo realiza el administrador?

Acciones correlativas a usuarios
• ¿Los usuarios se identifican en forma única o existen usuarios genéricos que todas las personas usan? ¿Todos los usuarios tienen un perfil o pertenecen a algún grupo?
• ¿Tienen forma de asignar responsabilidades individualmente a cada usuario, identificándolo a través de su ID?
• ¿Existen grupos de usuarios?

• ¿El acceso puede controlarse con el tipo de trabajo o la función (rol) del que pide acceso?
• ¿Los ID hacen referencia a una persona, o son anónimos? ¿Hacen referencia a un grupo?

Varios
• ¿Utilizan el ID de usuario como un control de acceso a los recursos, o solo para ingreso al sistema?
• ¿Un usuario puede tener solo una sesión abierta, de alguna aplicación, de acuerdo a sus tareas o puede tener varias? ¿Depende de la cantidad de grupos a los que pertenezca?
• ¿Qué tipos de perfil de administrador hay?
• ¿Cuántas personas y quiénes son administradores?
• ¿Desde qué terminal puede logearse un administrador?
• Además de la cuenta de administrador, ¿tienen otra cuenta para las funciones comunes?
• ¿Qué datos se muestran cuando alguien intenta logearse? ¿Se muestran los siguientes datos?
o Nombre de usuario
o Password
o Estación de trabajo
o Fecha y hora
• ¿Qué datos se muestran cuando alguien logra logearse? ¿Se muestran los siguientes datos?
o Fecha y hora de la última conexión.
o Localización de la última conexión (Ej. IP de terminal)
o Intentos fallidos de conexión de ese ID de usuario desde la última conexión lograda.

Datos de autenticación
• ¿Cómo se protegen los datos de autenticación cuando están siendo ingresados por el usuario? ¿Qué se muestra en pantalla cuando se tipea el password (Espacios, asteriscos, no se mueve el cursor).
• ¿Cómo se guardan los datos de autenticación en disco? ¿ cifrado de datos? ¿Bajo password? ¿De qué forma se los asegura?
• ¿Cómo se restringe el acceso a estos datos? ¿Hay un control de acceso más severo con estos datos? ¿Se los clasifica como confidenciales?
• ¿Quién tiene acceso a estos datos?
• ¿Cómo se transfieren los datos de autenticación desde la terminal que se logea hasta el servidor encargado de autenticar? ¿ Cifrado de datos, o solo en texto plano?
Alcance de la autenticación
• ¿Qué alcances tienen las autenticaciones? ¿Es una autenticación para una aplicación en particular o para toda la red?
Límites de los intentos de logeo
• ¿Se lockea el usuario después de varios intentos fallidos de autenticación o se inhabilita la cuenta o la terminal?
• ¿Después de cuantos intentos?
• ¿Qué se hace después de la inhabilitación: se espera un tiempo y muestra nuevamente la pantalla de logeo o el administrador debe aprobar la operación de re-logeo?
Varias
• Separación de tareas: ¿Se manejan los controles de acceso de manera que una sola persona no tenga acceso a todo, en relación a una sola transacción?
• ¿Existe separación de tareas a través del control de acceso?
• Rotación de tareas: si existe rotación de tareas, ¿cómo es el mecanismo

en el control de acceso para posibilitar esto? ¿Se modifican los permisos? ¿O tienen todos los permisos necesarios permanentemente?
• ¿Cómo se manejan con las passwords durante los períodos de vacaciones? ¿Qué ocurre con la cuenta del administrador en el período de vacaciones? ¿Puede ser modificada? ¿Cómo controlan que no sea modificada durante su ausencia?
Generación de Claves de Acceso
• ¿Las passwords son generadas con procesos automáticos (programas de generación de passwords) o son creadas por los usuarios? ¿Se usan estos programas en alguna máquina, por ejemplo en los servidores?
• ¿Qué características deben tener estas passwords?
○ ¿Cuál es el conjunto de caracteres permitidos.
○ ¿Cuál es el largo mínimo y máximo del password?
○ ¿La password se inicializa como expirada para obligar al cambio?
○ ¿De qué forma se hace cumplir este requerimiento?
○ ¿Se pone una fecha de expiración?
○ ¿No se al usuario logearse ya que su password ha expirado?
• ¿Se permite que contengan el nombre de la empresa, o el nombre del usuario?
• ¿Dos cuentas pueden tener las mismas passwords?
• Si existe más de una cuenta de administrador, ¿algunas de estas (o todas) tienen las mismas passwords?
• ¿El password puede ser igual al ID del usuario?
Cambio de Claves
• ¿Qué procedimiento existe para el cambio de las passwords de los usuarios?
• ¿Se puede cambiar en cualquier momento?
• ¿Quién puede hacer los cambios?

• ¿Tienen que avisar a alguien cuando cambian la contraseña?
• ¿Tiene que pedir autorización?
• ¿Cuál es el procedimiento para manejo de password perdidas o reveladas? ¿Cómo se cambian? ¿Solo se cambia la password o se cambia también la cuenta y el nombre del usuario?
• ¿Con qué frecuencia es necesario cambiar la password antes que se vuelva obsoleta?
• Al modificar la password de una cuenta, ¿se puede repetir la misma password?
• ¿Se guarda una base de datos con las últimas password de los usuarios?
• ¿Cuántas passwords de cada usuario se guardan?

TEMA: SEGURIDAD DE LAS APLICACIONES

Encuestados: Encargado de Redes y Jefe de Departamento

Elección del Sistema a Usar
• ¿Se hicieron cuestionarios al elegir los sistemas operativos y programas usados en la empresa?
• Para todo tipo de sistemas se tuvo en cuenta los siguientes requisitos:
○ Requerimientos funcionales
○ Entorno necesario.
○ Requerimientos de compatibilidad
○ Requerimientos de performance
○ Fiabilidad.
○ Precio y precio adicional de mantenimiento
○ Documentación y manuales propios del software
• Se tuvo en cuenta los siguientes requisitos de seguridad
○ Identificación y autenticación,

○ Control de acceso.
○ Login.
○ Incorruptibilidad.
○ Fiabilidad.
○ Back up de datos.
○ Cifrado de datos.
○ Funciones para preservar la integridad de datos.
○ Requerimientos sobre privacidad de datos.

CONTROL DE DATOS DE APLICACIONES
• ¿Existe un control de cambios para los archivos del sistema o para las bases de datos de la empresa, como por ejemplo una base de datos, que se modifique cada vez que alguien haga una modificación sobre un archivo?
• ¿Existen restricciones de datos de salida, por ejemplo al portapapeles o a la impresora, y otros?
• ¿Cómo es el acceso a las librerías de programa (o a la carpeta “Archivos de programa”)?
• ¿Se generan históricos de auditoría indicando qué procesos se corrigieron, quién los corrigió y qué cambios hizo (control de cambios – gestión de configuración)?
• ¿Los archivos de programa y los de trabajo se almacenen en directorios separados?

CONTROL DE APLICACIONES
• ¿Todas las máquinas de la empresa tienen los mismos programas con las mismas versiones?

• ¿Existe un estándar de configuración de PC´s a seguir?
• ¿Usan alguna herramienta para copiar la configuración de las PC's?
• ¿Existe un procedimiento para instalar las aplicaciones en las máquinas de los usuarios?
• ¿Quién los instala y administra?
• ¿Existen controles para realizar la instalación o la actualización de parches de las aplicaciones?
• ¿Cómo se documenta la instalación o actualización del software que se instala en las máquinas?
• ¿Existe algún procedimiento para encontrar programas que no deberían estar en las máquinas de los usuarios, ya sea por problemas de licencias o virus?
• ¿Existe un método a seguir? ¿Se usa algún producto para detectar estos programas? ¿Se hacen auditorías periódicas para verificar?
• ¿Cómo se controla a los usuarios y las aplicaciones que bajan de la web?
• ¿Cómo controlan que éstas tengan las licencias correspondientes (esto puede terminar en un problema para la empresa)?
• ¿Se borran las versiones de prueba (trial versión) o demos cuando expiran?
• ¿Se permiten los registros on line de las aplicaciones?
• ¿Existen métodos para autorizar y registrar software?
• ¿Cómo manejan las actualizaciones del software?
• ¿Existe alguna forma de configurar las PC´s de manera que no se pueda instalar software nuevo sin autorización del administrador?
• ¿Puede pasar que un usuario no esté autorizado para modificar las carpetas c:\Windows o c:\Archivos de programa, pero otro (el administrador de sistemas) sí? ¿Cómo se configura esto en el sistema de control de acceso de la empresa? ¿Se usa?

CONTROL DE DATOS EN EL DESARROLLO
• ¿Se asegura la integridad, exactitud y validez de los datos de entrada y salida de las aplicaciones?
• ¿Las variables, parámetros y / o fórmulas de cálculo se incluyen en tablas o archivos separados de los programas, para facilitar su modificación?
• ¿Existe un proceso de control de cambios para el desarrollo? ¿Cómo se documentan estos cambios?
• ¿Controlan el contenido de los archivos de entrada? ¿Controlan que existan los archivos antes de ejecutar el programa?
• ¿Se hacen controles sobre la validez de los datos ingresados manualmente? (Controles de integridad de datos)
• ¿Se controla la consistencia de los datos de salida de las aplicaciones?
• ¿Las aplicaciones se operan a través de menús obligatorios o es a través de comandos del sistema? ¿Los operadores de estas aplicaciones pueden editar los datos reales del mismo (o sea las bases de datos)?

CICLO DE VIDA
• ¿Qué aplicaciones se desarrollaron en la empresa? ¿Una para cada área de la empresa?
• ¿Qué metodología estándar usan para el desarrollo de sistemas? ¿De qué fases consta? ¿Qué mecanismos de seguridad manejan durante estas fases?
Iniciación
• ¿Cómo se expresan las necesidades del sistema?
Desarrollo
• ¿Se hace un análisis de riesgos antes de empezar con el desarrollo?
• ¿En caso de que haya participación de terceros en el desarrollo (como en

la web, o en LINUX) el código fuente queda en la empresa? ¿Dejan documentación? ¿Tienen alguna reglamentación para trabajar con terceros?
• ¿Usan métricas durante el desarrollo? ¿Les sirven? ¿Qué miden? ¿En qué las utilizan?
• ¿Se mantienen registros históricos de las modificaciones llevadas a cabo en los sistemas durante el desarrollo y el mantenimiento? ¿Qué se guarda?
○ sistema que afecta,
○ fecha de la modificación,
○ persona que realizó el cambio,
○ descripción global de la modificación,
○ ¿Qué más?
• ¿En qué momento se definen los requisitos de seguridad de un sistema? ¿Es durante el desarrollo?
Implementación
• ¿En qué lenguajes se implementan los sistemas? ¿Reusan software?
• ¿Qué medidas de seguridad toman durante la implementación?
Prueba
• ¿Cómo se hace la prueba de los sistemas?
• ¿Se generan planes de prueba?
• ¿Qué tipos de prueba se llevan a cabo? ¿De unidad? ¿De integración? ¿Por módulos? ¿Por sistema?
• ¿Se generan escenarios de prueba para el testeo?
• ¿Se documentan las pruebas y sus resultados? ¿Qué datos se guardan?
• ¿Cómo se realiza el control de cambios del sistema?
Instalación y mantenimiento
• ¿Qué metodología usan para el mantenimiento?

Documentación
• ¿Qué documentación generan de los desarrollos que hacen? ¿Se incluyen las siguientes cosas?
o Generalidades del sistema, incluyendo fecha de implementación y analista / programador responsable.
o Documentación del sistema, incluyendo sus objetivos, diagramas general y de funciones y diseños de registros.
o Documentación de los programas, incluyendo objetivos, diagrama de flujo y archivos de entrada y salida que utiliza.
o Manual de operación, que contenga el diagrama de flujo general de procesamiento donde se identifiquen los procesos que deben haber finalizado y las interfaces de entrada que se deben haber cubierto como paso previo a la ejecución de cada proceso, los procedimientos de supervisión, seguridad y control sobre los procesos y los pasos a seguir ante la ocurrencia de errores.
o Manual de usuario.
o Manual de características de seguridad.
o Descripción del hardware y software, políticas, estándares, procedimientos, backup, plan de contingencia, descripción del usuario y del operador del sistema.

TEMA: SEGURIDAD FÍSICA

Encuestados: Encargado de Redes y Jefe de Departamento

Control de acceso al Departamento de Informática
• ¿Se hizo un análisis costo beneficio a la hora de implementar los controles?
• Cómo se asesoraron?
• ¿Se restringe el acceso al centro de cómputos a la gente que no pertenece

a esa área?
• ¿Existen algunos de los siguientes métodos? ¿Dónde?
o tarjetas de entradas,
o guardias de Seguridad,
o circuito cerrado de televisión.
• ¿Cuál es la función de la doble puerta en la entrada?
• ¿Qué tipos de autenticación se utilizan en la empresa? Hay cuatro formas:
o con algo que el individuo sabe (password, PIN),
o algo que el individuo procesa (un token, una smart card.),
o algo que el individuo es (controles biométricos),
o algo que sabe hacer (como los patrones de escritura).
• ¿Por qué no usan las otras? ¿Por el costo? ¿No vale la pena?
• ¿Solo dejan entrar a aquellos que lo necesiten? ¿Les hacen algún control de seguridad?

CONTROL DE ACCESO A EQUIPOS
• ¿Cómo se controlan los siguientes accesos?
• ¿La BIOS tiene habilitada una contraseña?
• ¿Las PC's tienen habilitados los dispositivos externos, como la disquetera o la lectora de CD? ¿Cómo se controlan estos dispositivos?
• ¿Cómo se controlan los virus en las disqueteras o CD's? ¿Qué otros peligros pueden tener?
• ¿Son dispositivos booteables (se permite desde el setup de la máquina el booteo con estos dispositivos)?
• ¿Ha habido robo de datos usando estos dispositivos?
• ¿Existen copiadoras de CD's en la empresa? ¿Quién tiene acceso a ellas? ¿En qué máquinas están?
• ¿Usan llave de bloqueo en las CPU´s?

• ¿Las CPU´s y dispositivos externos extraíbles están guardados con llave?
• ¿Existe algún control sobre los terceros que realizan el mantenimiento?
• ¿Existen entradas no autorizadas en las PC's, como puertos no usados y no deshabilitados?
• ¿Puede alguien enchufar e instalar una impresora u otro dispositivo (un zip o un disco removible) en alguna máquina?
• ¿Cómo se realiza el control sobre los dispositivos que se instalan en las PC´s?
• ¿Se hace una revisión periódica de los mismos? ¿Quién las hace? ¿Cada cuanto? ¿Qué buscan?
• ¿Se apagan los servidores en algún momento? ¿Es necesario que queden en funcionamiento las 24 horas?

UTILIDADES DE SOPORTE
• ¿Existen, se mantienen y revisan todos estos aparatos periódicamente en busca de fallas?
• Aire acondicionado
• Calefacción
• Humidificador en la biblioteca de cintas y centro de cómputos
• Luz de emergencia en el centro de cómputos
• Detectores de humo, agua y calor
• Instalación de alarmas:
○ contra fuego,
○ humo,
○ calor,
○ intrusos,
○ agua,
○ ¿Qué otras hay?

• Servidor de repuesto o redundante
• UPS (Uninterruptible power supply) ¿para mantener los servidores de red funcionando por cuántas horas? ¿Cuántos UPS? ¿En qué máquinas?
• Estabilizador de tensión: ¿cuántos? ¿En qué máquinas?
• Extinguidores de incendio:
○ ¿Son los adecuados?
○ ¿Son manuales o automáticos (rociadores)?
○ ¿Se corta la energía eléctrica cuando se activan estos rociadores?
○ ¿Están en el lugar correcto? ¿En qué lugares? ¿Cómo eligieron el lugar?
○ ¿Se revisan las posibles fallas eléctricas o posibles causas de incendio?
○ ¿Qué pasa con las máquinas cuando cae la lluvia artificial? ¿Existen cubiertas plásticas para protección de agua?
○ ¿Qué pasa con los extinguidores de incendio en el centro de cómputos?
• ¿Hay una sola red eléctrica?
• ¿Hay un dispositivo que evite la sobrecarga de la red eléctrica?
• ¿Hay hardware especial de aislamiento y protección de dispositivos magnéticos?

ESTRUCTURA DEL EDIFICIO
• ¿Se tuvo en cuenta la seguridad de los datos y equipos en el momento de hacer la estructura de los edificios? ¿O se hizo primero la red y luego el edificio?
• Centro de cómputos:
○ ¿Está ubicado en pisos elevados (para prevenir inundaciones)?
○ ¿Existe un piso o techo falso para pasar el cableado por debajo de

él?
• ¿El área debajo del piso o del techo falso es fácilmente accesible?
○ ¿Es lo suficientemente grande, anticipándose al crecimiento de la red y predispuesto a reinstalaciones?
○ ¿La localización del centro de cómputos, tiene paredes externas o ventanas?
○ ¿Está cera del backbone (caño central de la red)?
○ ¿Esta permitido comer, fumar y beber dentro del centro de cómputos?
○ ¿En el resto de los escritorios se puede?
• ¿Los muebles son de madera? ¿Son inflamables?

CLASIFICACIÓN DE DATOS Y HARDWARE
• ¿Existen procesos para rotular, manipular y dar de baja la computadora, sus periféricos y medios de almacenamiento removibles y no removibles?
• ¿Cómo son estos procesos? ¿Con qué se rotulan los dispositivos?
• ¿Tienen un inventario de recursos de hardware y software? ¿Existe documentación sobre los dispositivos instalados en cada máquina, su configuración, modificación, forma de mantenimiento, versión?
○ ¿Cómo se guarda? ¿Es una planilla?
○ ¿Dónde se almacena?
○ ¿Quién lo actualiza?
○ ¿Cada cuanto?

BACKUP
• ¿Con qué frecuencia hacen los backups?
• ¿Qué datos se almacenan? (datos y programas de aplicación y de

sistemas, equipamiento, requerimientos de comunicaciones, documentación)
○ ¿Se hacen discos de inicio de Windows?
○ Software aplicativo,
○ Parámetros de sistema,
○ Logs e informes de auditorías,
○ Datos,
○ Backups del Hardware.
• ¿Hay backup especiales (con datos distintos, o particulares)? ¿Cada qué período de tiempo se hacen? ¿Qué datos guardan?
• ¿Qué tipo de back up hacen? (backups normales, backups incrementales, backups diferenciales) ¿En qué áreas o datos usan incrementales, en cuáles usan normales?
• ¿En qué medio se almacena? ¿Con qué dispositivo se hace?
• ¿Cómo es la rotación de los medios de backup? ¿En una semana, un mes?
• ¿Con qué aplicación se hacen? ¿Con algún tipo especial de aplicación de manejo de backup? ¿Es una del sistema operativo, del administrador de archivos u otra? ¿Utilizan archivos de tipo específicos o archivos .zip, por ejemplo?
• ¿Hay herramientas de back up automáticas, o sea que a través de una agenda hacen las copias?
• ¿Quién es el encargado o el responsable? ¿Los hace el administrador de sistemas?
• ¿Tienen formalizados los procedimientos de back up? ¿Existe un procedimiento escrito? ¿Si falta el responsable del backup, quién los hace?
• ¿Existen procedimientos escritos para recuperar archivos backupeados, o un Plan de backup?

• ¿Hacen pruebas periódicas de recuperación de backups?
• ¿Quién puede levantar los archivos de los usuarios, los backups de Mis Documentos, cualquier otro usuario?
• ¿Qué PC's o máquina es la que tiene mayor prioridad? ¿Cómo son las prioridades? ¿Según qué se determinó la prioridad de las máquinas: según un análisis de impacto, según la confidencialidad de la información?
• ¿Los backups se almacenan dentro y fuera del edificio? ¿Estos lugares son seguros?
• ¿Cómo se rotulan e identifican?
• ¿Hay documentación escrita sobre los backups hechos, sus modificaciones, fechas u otro tema?
• ¿Se necesita algún dispositivo (llaves, tarjeta) para entrar al almacén de cintas?
• ¿Se crean discos de inicio de Windows?
• ¿Hay información afuera de la red interna de la empresa que sea valiosa? ¿El web host tiene datos importantes de usuarios? ¿Se hacen backups de estos datos? ¿Dentro de la empresa o por el web host?
• ¿Hay backups de las páginas web y de sus actualizaciones?
• ¿Existen procedimientos automáticos para que, en caso que un usuario cometa un error en la base de datos, ésta pueda volverse a su estado anterior?
• ¿Cómo se hace?

TEMA: ADMINISTRACIÓN DEL CENTRO DE CÓMPUTOS

Encuestados: Jefe de Departamento

Organización del Departamento de Informática
• ¿Realizan un seguimiento de todos los archivos logísticos a fin de detectar

cambios en las estadísticas obtenidas (realizados en comparación con los archivos del mes anterior, por ejemplo)?
• ¿Existe un programa que haga estas comparaciones? ¿Se usa? ¿Da buenos resultados?
• ¿Existen procedimientos para dar publicidad a las nuevas normas de seguridad?
• ¿Cómo harían el aviso de las políticas de seguridad?
• ¿Con charlas o reuniones?
• ¿Exposición en transparencias?
• ¿Por una notificación expresa a cada empleado?
• ¿Cómo funciona el boletín mensual que les entregan a los usuarios? ¿Qué temas trata?
• ¿Se entrena a los usuarios y administradores? ¿Quién es el encargado? ¿Por qué?
• ¿Se tienen en cuenta los delitos no tecnológicos? (Ej.: discutir temas privados de la organización en lugares no aptos, ingeniería social, entre otros)
• ¿Existe algún tipo de mesa de reportes donde los usuarios con incidentes de seguridad pueden recibir ayuda o realizar un reporte?
• ¿Existe un Plan de Sistemas formal? (plan a corto plazo de actividades del Departamento)
• ¿Quién los hace?
• ¿En base a qué estudios definen las cosas por hacer?
• ¿Existe un Plan Estratégico de Sistemas? (plan a largo plazo de proyectos)
• ¿Existen políticas, normas, estándares y procedimientos que sirvan como base para la planificación, el control y la evaluación de las actividades del área de sistemas de información?
• ¿Existe una planificación y documentación escrita y actualizada de las

actividades que se desarrollan normalmente en el centro de procesamiento de información?
• ¿Existe documentación detallada sobre el equipamiento informático?
• ¿Se tienen en cuenta tanto al centro de procesamiento de datos principal como de los secundarios, redes departamentales, sucursales y al centro alternativo para contingencias?
• ¿Se actualiza la lista de activos?
• ¿Existe algún manual de seguridad, para el personal de seguridad o para los usuarios?
• ¿Es automático el método de actualización de los antivirus para que los mensajes internos en el interior y el exterior de la organización no propaguen virus? ¿Se programan los escaneos automáticos de virus? ¿Cada cuanto tiempo? ¿Por qué no se actualiza la aplicación automáticamente con un schedule?
• ¿Cómo se etiquetan y almacenen los instaladores de los programas o los drivers? ¿Se almacenan en disco duro, en DVD, en cinta?
• ¿Se borran los archivos de las carpetas temporales, para que no se llenan los discos de basuras y provoquen la caída del sistema?
• Todas estas tareas ¿Son realmente útiles? ¿Se dan en la práctica?

RESPONSABILIDAD DEL EQUIPO DE SEGURIDAD
• ¿Cómo se administran las emergencias? ¿Si se hacen cambios de emergencia, cómo se documenta?
• ¿Quién es el encargado de la seguridad? ¿Y de una política de seguridad y su administración?
• ¿Quién se encarga de administrar la estructura de seguridad una vez implementada?

• ¿Existe un solo responsable del centro de cómputos?
• ¿Qué privilegios (o accesos) se le dan a las personas recién contratadas en el centro de cómputos?
• ¿Cuál es la diferencia de permisos entre los desarrolladores y los administradores?
• ¿Quién asigna los permisos a los distintos roles o grupos?
• ¿Quién es el encargado de informar a los ejecutivos de la empresa sobre la administración de seguridad, actividad de seguridad de la información, y riesgos? ¿Se realizan informes periódicos? ¿Son a pedido de alguien o a modo de auto evaluación?
• ¿Quién es el encargado de recomendar la separación de tareas y responsabilidades para las funciones de IT?
• ¿Quién es responsable de asegurar que los sistemas de seguridad física están en su lugar?
• ¿Existe en los empleados y altos ejecutivos una conciencia sobre su importancia de la seguridad?
• Todas estas tareas ¿Son realmente útiles? ¿Se dan en la práctica?

AUDITORÍAS Y REVISIONES
Auditorías Generales
• ¿Se hacen auditorías en la empresa?
• ¿Qué objetos se auditan? Para cada clase de objetos, ¿qué accesos se auditarán?
○ Archivos y directorios
○ Claves del registro
○ Servicios
○ Impresoras
• ¿Qué actividades se monitorizan?

• Monitorización del sistema general
• Monitorización de reinicio de los sistemas
▪ Monitorización de fallas de hardware
▪ Monitorización de procesos
▪ Monitorización de aplicaciones
• ¿Qué otra clase de eventos se auditarán?
• ¿Se hacen chequeos aleatorios para verificar el cumplimiento de los requerimientos y procedimientos de seguridad? ¿Sería útil?
• ¿Cuánto se monitoriza? (Monitorizar tiene un impacto directo en la performance del sistema) ¿Cómo hacen para que los recursos alcancen?
• ¿Qué pasa con la información que se obtiene de las auditorías?
• ¿Las auditorías permiten rastrear las acciones de cada usuario?
• ¿Que se audita?
• ¿Se audita según las acciones, las maquinas o los usuarios?
• ¿Cada uno de estos activos en particular o depende de los sectores y/o máquinas y/o sensibilidad de la información?
• ¿Las auditorías soportan investigaciones luego de los hechos, con datos sobre cómo, cuándo y por qué cesaron las operaciones normales?
• ¿Se reúne información de las auditorías para formar perfiles de los usuarios del sistema? ¿Observan, por ejemplo, patrones en los usuarios, como las terminales que utilizan, horas de acceso, y permisos que solicitan, para determinar qué acciones son inusuales y deben ser investigadas?
• ¿Se usan herramientas automáticas para revisar los registros de auditorías en tiempo real?
• ¿Se generan históricos de auditoría indicando qué procesos se corrigieron, quién los corrigió y qué cambios hizo (control de cambios – gestión de configuración)?

• ¿Se investiga la actividad sospechosa? ¿Se toman acciones?
• ¿Se documentan la ejecución y los resultados de estas pruebas?

RESPONSABILIDADES DE LOS ENCARGADOS DE SEGURIDAD
• ¿Quién administra, desarrolla e implementa los procedimientos de auditoría y revisión? ¿Quién conduce la auditoría?
• ¿Quién selecciona los eventos de seguridad a ser auditados?
• ¿Quién administra la documentación sobre los resultados?
• ¿Quién se encarga de monitorizar y reaccionar a los avisos (warnings) y reportes?
• ¿Quién hace chequeos aleatorios para verificar el cumplimiento de los requerimientos y procedimientos de seguridad?
• ¿Quién se encarga de reunir datos de las auditorías para formar perfiles de los usuarios del sistema?
• ¿Quién revisa los reportes de auditorías buscando anomalías?
• ¿Hay separación de tareas entre los que administran el control de acceso y los que hacen las auditorías, o son las mismas personas?
• ¿Quién se encarga de buscar nuevas herramientas que faciliten la auditoría?

TEMA: AUDITORÍA

Encuestados: Jefe de Departamento

AUDITORÍAS DE CONTROL DE ACCESO
• ¿Se generan logs de auditoría del control de acceso?
• ¿Cuándo se almacenan, ante qué eventos? ¿Se almacenen cuando ocurre alguno de estos eventos?
○ Login exitoso

○ Login fallido
○ Procedimientos de cambios de passwords satisfactorio
○ Procedimientos de cambios de passwords fallido
○ Lockeo de un usuario
○ Modificación en bases de datos
○ Utilización de herramientas del sistema
○ Modificación de ciertos datos (como datos de configuración, datos críticos, datos de otros usuarios)
○ Acceso a Internet
○ Alertas de virus
• ¿Dónde se almacenan?
• ¿Quién tiene acceso a los logs?
• ¿Por cuánto tiempo permanecen guardados?
• ¿Se borran cuando expira ese tiempo o se genera una estadística comprimida de los mismos y de guarda un análisis de ellos solamente?
• ¿Qué datos se almacenan en los logs? ¿Se almacenan los siguientes datos?
• Para todos los eventos:
• Fecha y hora del evento
• Tipo de evento (Ej. Login, modificación de datos)
• ID de usuario
• Origen del evento (Ej. Terminal Nº 9)
○ Acceso a Internet:
• Páginas visitadas
• Cookies guardadas
• Archivos descargados
• Servicios utilizados
• Aplicaciones utilizadas

○ Modificación de ciertos datos
• Datos modificados
• Valor anterior
• ¿Por cuánto tiempo se guarda el valor anterior de los datos?
• ¿Se hace alguna comprobación antes de efectuar el cambio definitivo?
• ¿Qué se hace si se modifica algún valor de la configuración del sistema?
• ¿Las estadísticas que genera son buenas? ¿Faltan datos por analizar que son importantes para la administración del control de acceso?

SEGURIDAD DE REDES Y ACCESO A INTERNET
• ¿Cómo es la topología de la red?
• ¿Qué dispositivos tienen en la red:
• switch,
• routers,
• hub's,
• PC's,
• fibra óptica.
▪ ¿Cuántos dispositivos de esta lista hay y en qué forma están ubicados y utilizados?
▪ ¿Cómo está conectada la red?
• ¿Se hace algún chequeo periódico de la red y sus permisos?
• ¿Qué se controla?
• ¿Se documentan la ejecución y los resultados de estas pruebas?
• ¿Cómo se utiliza internet en la empresa?
• ¿Cómo se administra el correo en el servidor y cómo se hace?
• ¿El servidor de mail es el mismo que el servidor de Internet?

Formulario descriptivo del Trabajo Final de Graduación

Este formulario estará completo sólo si se acompaña de la presentación de un resumen en castellano y un abstract en inglés del TFG

El mismo deberá incorporarse a las versiones impresas del TFG, previa aprobación del resumen en castellano por parte de la CAE evaluadora.

Recomendaciones para la generación del "resumen" o "abstract" (inglés)

“Constituye una anticipación condensada del problema que se desarrollará en forma más extensa en el trabajo escrito. Su objetivo es orientar al lector a identificar el contenido básico del texto en forma rápida y a determinar su relevancia. Su extensión varía entre 150/350 palabras. Incluye en forma clara y breve: los objetivos y alcances del estudio, los procedimientos básicos, los contenidos y los resultados. Escrito en un solo párrafo, en tercera persona, contiene únicamente ideas centrales; no tiene citas, abreviaturas, ni referencias bibliográficas. En general el autor debe asegurar que el resumen refleje correctamente el propósito y el contenido, sin incluir información que no esté presente en el cuerpo del escrito.

Debe ser conciso y específico”. Deberá contener seis palabras clave.

Identificación del Autor

Apellido y nombre del autor:	CARACINO JOSE LUIS
E-mail:	jcaracino@msn.com
Título de grado que obtiene:	Licenciatura en Informática

Identificación del Trabajo Final de Graduación

Título del TFG en español	Aplicación de Normas ISO 17799 y COBIT de la Seguridad Lógica en la Empresa Agua de los Andes S.A.
Título del TFG en inglés	Implementation of ISO 17799 and COBIT rules of Logic Security in Agua de los Andes SA Company
Tipo de TFG (PAP, PIA, IDC)	Proyecto de Aplicación Profesional (PAP)
Integrantes de la CAE	Ing. Jorge Cassi / Ing. Mario Groppo
Fecha de último coloquio	01/06/2012

con la CAE	
Versión digital del TFG: contenido y tipo de archivo en el que fue guardado	seguridadlogica.PDF

Autorización de publicación en formato electrónico

Autorizo por la presente, a la Biblioteca de la Universidad Empresarial Siglo 21 a publicar la versión electrónica de mi tesis. (Marcar con una cruz lo que corresponda)

Autorización de Publicación electrónica:

- ☐ **Si, inmediatamente**
- ☐ **Si, después de ….. mes(es)**
- ☐ **No autorizo**

Firma del alumno