UNIVERSIDAD DEL AZUAY
FACULTAD CIENCIAS DE LA ADMINISTRACION
ESCUELA DE SISTEMAS Y TELEMÁTICA

Auditoría de la Gestión de Seguridad Informática de la Unidad Educativa Particular "La Asunción" basada en COBIT 5

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERA EN SISTEMAS Y TELEMÁTICA

Nombre: Jessica Uyaguari Chalco

Director: Ing. Esteban Crespo Martínez

CUENCA -ECUADOR
2015

DECLARACIÓN

Yo, Jessica Paola Uyaguari Chalco, declaro por honor y bajo mi propia ética que el contenido del presente documento, previo a la titulación de Ingeniera en Sistemas y Telemática es de mi autoría; que no ha sido anteriormente presentado en otro trabajo de titulación o de algún ámbito profesional; y que he consultado en las referencias bibliográficas citadas en este documento.

Jessica Paola Uyaguari Chalco.

AGRADECIMIENTOS

Quiero dejar constancia de mi profundo agradecimiento a la Institución Educativa Particular “La Asunción”, por brindarme la facilidad para la realización de este trabajo, así como también al Ing. Esteban Crespo, director de tesis, por ser un excelente profesional, con capacidad de conducción y liderazgo, que impulsó el desarrollo de este trabajo de Auditoría.

Finalmente a mis padres por ser el principal cimiento para la construcción de mi vida profesional y por su apoyo incondicional en mis deseos de superación.

DEDICATORIA

A Dios
Que me ama y vela por mí, bendiciéndome con salud y sabiduría para alcanzar mis metas.

A mis padres Gabriel y Olga y mi hermana Denisse
Por su apoyo incondicional y sacrificios realizados para mi superación personal y profesional. Les amo mucho.

A mi esposo Santiago
Por su amor, apoyo y compañía en el transcurso de la realización de esta tesis. Te amo.

A mi hija Rafaela
Dejo constancia que mi hija fue mi principal motivación para la realización de este trabajo y la bendición más grande que Dios me regalo.

A mis familiares y amigos
A toda mi familia que llevo en mi corazón y siempre están conmigo; especialmente a mi abuelita Chocha que desde el cielo vela por mí y comparte esta gran alegría. Te extraño abuelita.

Contenido

Tabla de Ilustraciones

RESUMEN

El presente trabajo de titulación: “Auditoría de la Gestión de Seguridad Informática de la Unidad Educativa Particular “La Asunción” basada en COBIT 5”; aplica los fundamentos teóricos de la seguridad en Redes de Datos, además de la metodología COBIT, los mismos que han permitido realizar un estudio sobre la situación actual de la institución en cuanto a la parte administrativa e infraestructura tecnológica; para luego con los habilitadores de seguridad de COBIT respectivos, poder planificar y desarrollar una Auditoría informática.

Finalmente se dan a conocer los resultados del proceso de Auditoría, detallando los más relevantes de la misma y emitiendo las recomendaciones pertinentes.

ABSTRACT

This graduation work entitled "Management Auditing of IT-Information Security at *La Asuncion* private school, based on COBIT 5", applies, in addition to the COBIT methodology, the theoretical foundations of security in data networks. Therefore, these enabled us to conduct a study on the current situation of the institution in terms of the administrative and technological infrastructure in order to plan and develop an IT auditing with the respective COBIT security enablers.

Finally, we will inform the results of the auditing process, detailing the most important parts, and presenting the appropriate recommendations.

UNIVERSIDAD DEL AZUAY
Dpto. Idiomas

Translated by,
Lic. Lourdes Crespo

CAPÍTULO 1

FUNDAMENTOS GENERALES

Seguridad de Redes COBIT como metodología

1.1 Historia Estándar COBIT como metodología

"ISACA comenzó en 1967, cuando un pequeño grupo de personas con trabajos similares auditar controles en los sistemas computacionales que se estaban haciendo cada vez más críticos para las operaciones de sus respectivas organizaciones—se sentaron a discutir la necesidad de tener una fuente centralizada de información y guías en dicho campo. En 1969, el grupo se formalizó, incorporándose bajo el nombre de EDP Auditors Association (Asociación de Auditores de Procesamiento Electrónico de Datos).

En 1976 la asociación formó una fundación de educación para llevar a cabo proyectos de investigación de gran escala para expandir los conocimientos y el valor en el campo de gobierno y control de TI. Conocida previamente como la Information Systems Audit and Control Association (Asociación de Auditoría y Control en Sistemas de Información), ISACA ahora es solo un acrónimo, que refleja la amplia gama de profesionales en gobierno de TI a los que sirve." (ISACA, 2014).

Según el artículo publicado en el internet de (ISACA, 2014) "ISACA fue conformada por personas que reconocieron la necesidad de contar con una fuente centralizada de información y guías en el creciente campo de la Auditoría a los controles de los sistemas computacionales. Hoy, ISACA tiene más de 115,000 miembros en todo el mundo."

Según (COBIT) (Control Objetives Information Tecnologies - Objetivo de Control para Tecnología de Información), constituye la tercera edición de los Objetivos de Control en el cual el editor principal fue el Instituto de Gobierno de TI, el mismo que creo una herramienta de Gobierno de TI, que vincula la tecnología informática y prácticas de control, además consolida estándares de fuentes globales confiables en un recurso esencial para la administración (gerencia), los usuarios (profesionales de control) y los auditores.

Se puede concluir diciendo que COBIT está basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

1.2 Misión

(ISACA, 2012) Señala que esta nueva versión de Cobit 5 fue desarrollada para ayudar a organizaciones de todos los tamaños y de cualquier sector a obtener el valor óptimo de las tecnologías de información, tratando de satisfacer las necesidades de los interesados internos y externos mediante la creación de valor para la empresa a través de TI (tecnologías de información), con un enfoque de gestión holística de extremo a extremo, cumpliendo de mejor manera con leyes, regulaciones, políticas, y basándose en buenas prácticas internacionales.

“

Ser el referente en la Auditoría, Seguridad y Control de los SI / TIC en la Sociedad y ante las Autoridades.
Generar un beneficio mantenido de servicios a nuestros asociados.
Fomentar la formación continuada de los miembros de la Asociación.
Promover la participación activa de los asociados, a través de la Asociación (Comisiones de trabajo, normas técnicas, formación, etc.).”

1.3 Alcance

“Orientado al negocio (Gerencia).
Alineado con estándares y regulaciones de hecho y de derecho.
Basado en normas revisadas crítica y analíticamente para ser aceptadas en las tareas y actividades de TI.
Alineado con estándares de control y Auditoría (COSO, IFAC, IIA, ISACA, AICPA).
Aplicable a las funciones de Servicios de Sistemas de Información de toda la empresa.” (COBIT)

1.4 Gestión de seguridad de redes.

1.4.1 Introducción

En sociedad actual la mayoría de las empresas no destinan sus inversiones en seguridad a la hora de comprar productos (hardware y software). Un porcentaje muy bajo de empresas busca seguridad y calidad en los productos a la hora de comprar; pero el otro porcentaje faltante busca abaratar su inversión no considerando ni la calidad ni la seguridad del software y hardware.

Otras empresas descuidan el hardware y software, pero asignan parte de su presupuesto a la gestión de la seguridad de la información. El concepto de seguridad está variando, considerando ahora el concepto de seguridad gestionada.

1.4.2 Gestión de Redes

Según señala (Orozco) en su libro Gestión de la Red 3 se puede definir como gestión de la red a la Planificación, organización, supervisión y control de elementos de comunicaciones y recursos humanos para garantizar un nivel de servicio y de acuerdo a un coste.

La gestión de la red tiene como objetivos principales:

- Garantizar un servicio continuo
- Capacidad para superar o evitar fallas
- Capacidad para monitorear y diagnosticar condiciones no satisfactorias
- Monitoreo del rendimiento esperado
- Expansión y reconfiguración dinámica
- Mejorar la seguridad de la red.
- Manejo Integrado de la red
- Centralización de la gestión con implementación distribuida

- Reducir costo operacional de la red
- Incrementar la flexibilidad de operación e integración.
- Fácil uso de la red.

(Herrera) Señala los que La gestión de una red involucra varios puntos referentes a la ejecución de funciones y las herramientas útiles para realizarlas, de tal manera que existen los siguientes Procesos y Procedimientos definidos:

La Gestión de Configuración
La Gestión de Fallas
La Gestión del Rendimiento de la red
La Gestión de Seguridades
La Gestión de Planificación, y
La Gestión de Carga y Confiabilidad

1.4.3 Gestión de Seguridad

Según el libro SISTEMA DE GESTIÓN DE REDES Y SERVICIOS DE TELECOMUNICACIONES de (TELECOMUNICACIONES IV) la gestión de seguridad se refiere básicamente a los mecanismos de que dispone el administrador de una red para monitorear los recursos, los permisos de uso de estos recursos asignados a usuarios y el uso en sí que se le da a estos.

"La misión de la gestión de seguridad es ofrecer mecanismos que faciliten el mantenimiento de políticas de seguridad (orientadas a la protección contra ataques de intrusos)." (SISTEMA DE GESTIÓN DE REDES Y SERVICIOS DE TELECOMUNICACIONES).

Se relaciona con 2 aspectos de la seguridad del sistema:

La gestión de seguridad misma, que se refiere a la habilidad para supervisar y controlar la disponibilidad de facilidades de seguridad, y a reportar amenazas y rupturas en la seguridad.

Y la seguridad de la gestión, que requiere de la habilidad para autentificar usuarios y aplicaciones de gestión, para así garantizar la confidencialidad e integridad y prevenir accesos no autorizados a la información.
Para cumplir satisfactoriamente con la realización de estas tareas, es necesario tomar en consideración ciertas políticas de seguridad.

1.4.3.1 Políticas de seguridad

Definición: "El objetivo de la Política de Seguridad de una organización es, por un lado, mostrar el posicionamiento de la organización con relación a la seguridad, y por otro lado servir de base para desarrollar los procedimientos concretos de seguridad." (Mifsud, 2012)

A opinión de (Mifsud, 2012) indica que la empresa debe disponer de un documento formalmente elaborado y aprobado sobre el tema y que debe ser divulgado entre todos los empleados.
Este documento deberá lograr la concienciación, entendimiento y compromiso de todos los involucrados.
Con respeto a las políticas detalladas en el informe deben contener claramente las prácticas que serán adoptadas por la compañía u empresa. A su vez estas políticas deben ser revisadas, y si es necesario actualizadas, periódicamente.
Sin embargo, la seguridad debe ir más allá del conocimiento de los empleados y cubrir las siguientes áreas:

Un mecanismo de seguridad física y lógica que se adapte a las necesidades de la compañía y al uso de los empleados.
Un procedimiento para administrar las actualizaciones.
Una estrategia de realización de copias de seguridad planificada adecuadamente.
Un plan de recuperación luego de un incidente.
Un sistema documentado actualizado.

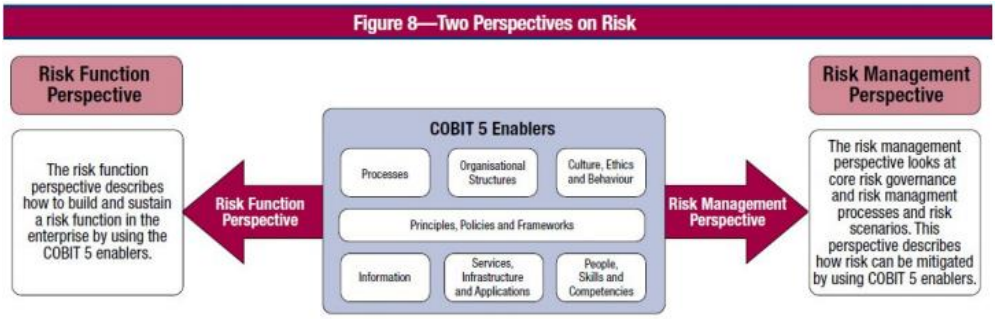
1.4.3.2 Riesgos Informáticos

Definición: (ISACA, 2012) Para riesgos define el riesgo de TI como un riesgo de negocios, específicamente, el riesgo de negocios asociado con el uso, la propiedad, la operación, el involucramiento, la influencia y la adopción de TI dentro de una empresa.

"El análisis de Riesgos trata sobre como minimizar los efectos de un problema de seguridad; para esto se debe tener identificado claramente qué es lo se quiere proteger, contra qué, y cómo se lo va a proteger.
Se conocen dos alternativas para responder a estas inquietudes, una cuantitativa y otra cualitativa. (A, 2012).

(ISACA, 2012) En su libro señala que COBIT hace uso de dos perspectivas de riesgo:

Perspectivas de la Función de Riesgo
"Describe lo que se necesita en una empresa para construir y sostener actividades efectivas de gobierno y gestión de riesgos."
Perspectiva de la Administración de Riesgo
"Describe como los procesos "core" de gestión de riesgos que son identificación, análisis, respuesta y respuesta de riesgos, pueden ser apoyadas con los habilitadores de COBIT 5"



(ISACA, 2012) Pag. 13

1.4.3.3 Identificación de Recursos:

Recursos cuya identidad puede ser amenazada:

Hardware
Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadores, personales, impresoras, unidades de disco, líneas de comunicación, servidores, routers.
Software
Códigos fuente y objeto de aplicaciones, utilidades, programas de diagnóstico, sistemas operativos, programas de comunicación, aplicaciones cliente-servidor.
Información
En ejecución, almacenada en línea, almacenada fuera de línea, en comunicación, bases de datos.
Personas
Usuarios, operadores, administradores.
Accesorios
Papel, cintas, tóners, CD´s.

1.5 Estructura del estándar COBIT

El estándar consta de un conjunto de Herramientas y Guías para ejecutar la implementación, soportar la administración y para alcanzar los objetivos planteados por la Administración, Usuarios y Auditores.

Resumen Ejecutivo.
Marco de Referencia.
Objetivos de Control.
Guías de Auditoría.
Herramientas de Implementación.
Guías de Administración.

1.5.1 Resumen Ejecutivo

(ISACA, 2012) Se refiere a la información como un recurso clave para todas las empresas, desde se crea hasta que es destruida; en la cual la tecnología juega un papel importante. La

tecnología de la información está avanzando cada vez más y se ha generalizado en las empresas y en entornos sociales, públicos y de negocios.

Actualmente según (ISACA, 2012) las empresas y sus ejecutivos se esfuerzan en:

Mantener información de alta calidad para soportar las decisiones del negocio.

Generar valor al negocio con las inversiones en TI, por ejemplo, alcanzando metas estratégicas y generando beneficios al negocio a través de un uso de las TI eficaz e innovador.

Alcanzar la excelencia operativa a través de una aplicación de la tecnología fiable y eficiente.

Mantener los riesgos relacionados con TI en un nivel aceptable

Optimizar el coste de los servicios y tecnologías de TI

Cumplir con las constantemente crecientes leyes, regulaciones, acuerdos contractuales y políticas aplicables.

Como resultado las empresas de éxito han reconocido que el comité y los ejecutivos deben aceptar las TI como cualquier otra parte importante de hacer negocios. Los comités y la dirección tanto en funciones de negocio como de TI deben colaborar y trabajar juntos, de modo que se incluya la TI en el enfoque del gobierno y la gestión. Además, cada vez se aprueba más legislación y se implementan regulaciones para cubrir esta necesidad.

1.5.2 Marco de referencia

Según (ISACA, 2012) COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas.
Se puede decir que COBIT ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.
COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público.

Dentro del marco de referencia vale recalcar que (ISACA, 2012) en su libro indica que COBIT se basa en cinco principios claves para el gobierno y la gestión de las TI empresariales como se muestra en la Ilustración 1-1.

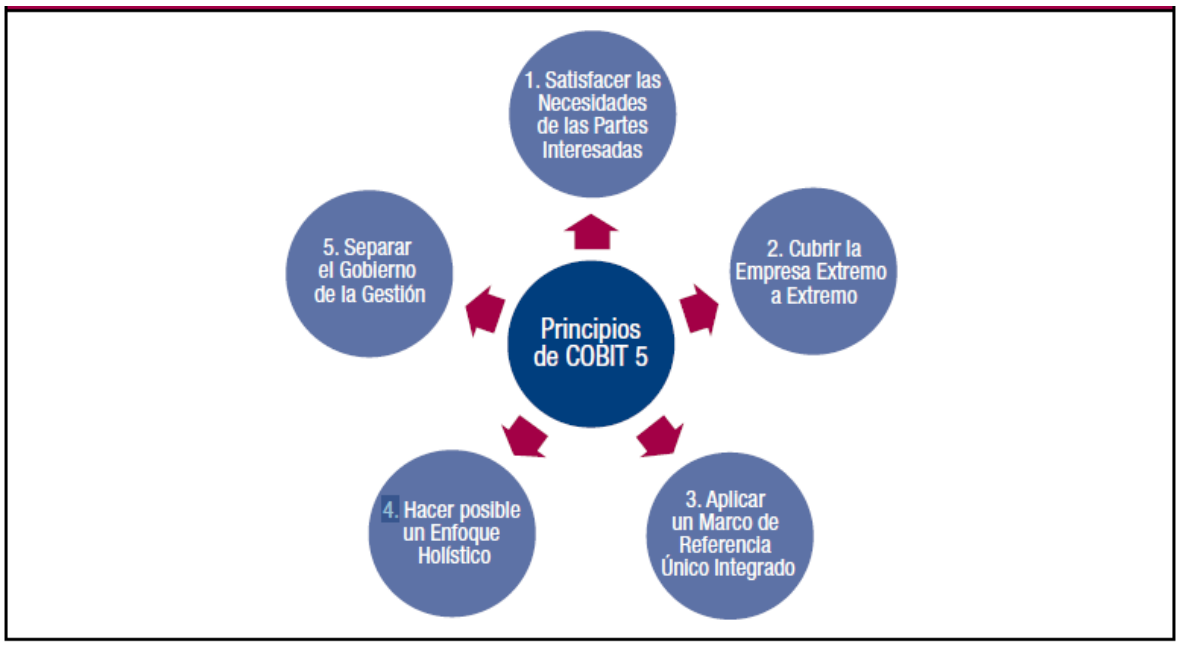


Ilustración 1-0-1Principios de COBIT 5

Principios de COBIT

Los principios que a continuación se citan provienen de (ISACA, 2014)

1. **Satisfacer las necesidades de las partes Interesadas**

   Las compañías existen para crear valor a sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos.

Ilustración 1-2Principio 1 (ISACA, 2014)

El sistema de gobierno deberá considerar para cada decisión, hacer las siguientes preguntas:

¿Quién recibe los beneficios?
¿Quién asume el riesgo?
¿Qué recursos se necesitan?

2. Cubrir la Empresa Extremo-a-Extremo

En este principio COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo es decir:

- Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no se enfoca sólo en la "función de TI", sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa. (ISACA, 2012).
- Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos los internos externos, los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas. (ISACA, 2012).

3. Aplicar un Marco de Referencia único integrado

COBIT 5 está alineado con los últimos marcos y normas relevantes usadas por las organizaciones y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las Ti de la empresa:

- Corporativo: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000.
- Relacionado con TI: ISO/IEC 38500, ITIL, la serie ISO/IEC 27000, TOGAF, PMBOK/PRINCE2, CMMI, etc.

Así se permite a la Organización utilizar COBIT 5 como integrador macro en el marco de gobierno y administración.
ISACA está desarrollando el modelo de capacidad de los procesos para facilitar al usuario de COBIT el mapeo de las prácticas y actividades contra los marcos y normas de terceros.

4. Hacer Posible un Enfoque Holístico

COBIT 5 define un conjunto de catalizadores *(enablers)* para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Definiendo a catalizadores como cualquier cosa que puede ayudar a conseguir las metas de la empresa. Descritos por el marco de COBIT 5 en siete categorías:

- Principios, Políticas y Marcos de Trabajo: "Son los vehículos para traducir el comportamiento deseado en una orientación práctica para la administración diaria."
- Procesos: "Describen una serie organizada de prácticas y actividades para lograr determinados objetivos y producir una serie de resultados como apoyo al logro de las metas globales relacionadas con la TI"
- Estructuras Organizativas: "Constituyen las entidades claves para la toma de decisiones en una organización."
- Cultura, Ética y Comportamiento: "De los individuos así como de la organización; se subestima frecuentemente como factor de éxito en las actividades de gobierno y administración."
- Información: "Se encuentra presente en todo el ambiente de cualquier organización; o sea se trata de toda la información producida y usada por la Organización. La información es requerida para mantener la organización andando y bien gobernada, pero a nivel operativo, la información frecuentemente es el producto clave de la organización en sí."

- Servicios, Infraestructuras y Aplicaciones: "Incluyen la infraestructura, la tecnología y las aplicaciones que proporcionan servicios y procesamiento de tecnología de la información a la organización."
- Personas, Habilidades y Competencias: "Están vinculadas con las personas y son requeridas para completar exitosamente todas las actividades y para tomar las decisiones correctas, así como para llevar a cabo las acciones correctivas."

5. Separar el Gobierno de la Gestión

Para su definición comenzaremos separando los términos de:

- Gobierno: En la mayoría de las organizaciones el Gobierno es responsabilidad de la Junta Directiva bajo el liderazgo de su Presidente.
- Gestión: En la mayoría de las organizaciones, la Administración es responsabilidad de la Gerencia Ejecutiva, bajo el liderazgo del Gerente General *(CEO)*.
  La gerencia también contiene cuatro dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar *(Plan, Build, Run and Monitor - PBRM)*.

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

Podemos observar que estas dos disciplinas: Comprenden diferentes tipos de actividades, requieren diferentes estructuras organizacionales y cumplen diferentes propósitos. Como se puede observar en la Ilustración 1-3.

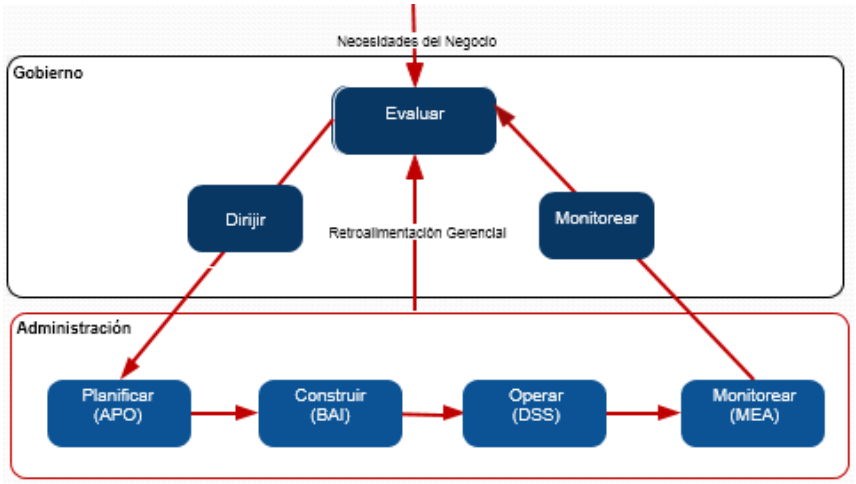


Ilustración 1-3Gobierno-Administracion (ISACA, 2014)

Dominios de COBIT 5

Estos dominios son una evolución de la estructura de procesos y dominios de COBIT 4.1: (Gobernance Institute (IT), 2007)

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

   "APO cubre las estrategias y las tácticas, identificando de la mejor manera en que TI puede contribuir al logro de los objetivos del negocio. En el cual la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Se debe implementar una estructura organizacional y una estructura tecnológica apropiada.
   Los siguientes cuestionamientos típicos de la gerencia cubren este dominio:

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

   Finalmente este dominio proporciona dirección para la entrega de soluciones *(BAI)* y la entrega de servicio *(DSS)"* (ISACA, 2012)

2. **Construir, Adquirir e Implementar (Build, Acquire and Implement, BAI)**

   "Las soluciones de TI necesitan ser implementadas e integradas así como identificadas, desarrolladas o adquiridas los procesos del negocio. Este dominio también cubre el cambio y el mantenimiento de los sistemas existentes para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.
   Los siguientes cuestionamientos de la gerencia cubren este dominio:

   ¿Es probable que los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio?
   ¿Es probable que los nuevos proyectos sean entregados a tiempo y dentro del presupuesto?
   ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?
   ¿Los cambios no afectarán a las operaciones actuales del negocio? (ISACA, 2012)

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

   "Cubre la entrega en sí de los servicios requeridos, el cual incluye: la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativos.
   Cubre las siguientes preguntas de la gerencia:

   ¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio?
   ¿Están optimizados los costos de TI?
   ¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?
   ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

   Finalmente se puede decir que recibe las soluciones y las hace utilizables por los usuarios finales." (ISACA, 2012).

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

   "Evaluar de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control todos los procesos de TI. Este dominio comprende la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.
   Abarca las siguientes preguntas de la gerencia este dominio:

   ¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde?
   ¿La Gerencia garantiza que los controles internos son efectivos y eficientes?
   ¿Puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio?
   ¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño?" (ISACA, 2012).

A lo largo de estos cuatro dominios, COBIT ha identificado 37 según (ISACA, 2012) procesos de TI generalmente usados, para cada uno de estos procesos define Objetivos de Control.

Objetivos de Control

Según (Gobernance Institute (IT), 2007) los objetivos de control de TI proporcionan un conjunto completo de requerimientos de alto nivel a considerar por la gerencia para un control efectivo de cada proceso de TI.
Ellos:

- Son sentencias de acciones de gerencia para aumentar el valor o reducir el riesgo.
- Consisten en políticas, procedimientos, prácticas y estructuras organizacionales.
- Están diseñadas para proporcionar un aseguramiento razonable de que los objetivos de negocio se conseguirán y que los eventos no deseables se prevendrán, detectarán y corregirán.

La gerencia de la empresa necesita tomar decisiones relativas a estos objetivos de control:

- Seleccionando aquellos aplicables.
- Decidir aquellos que deben implementarse.
- Elegir como implementarlos (frecuencia, extensión, automatización, etc).
- Aceptar el riesgo de no implementar aquellos que podrían aplicar.

Guías de Implementación

(ISACA, 2012) Indica que para obtener un valor óptimo aprovechando COBIT es necesario adaptarlo de manera eficaz para ajustarse al entorno único de cada empresa. Para ello cada enfoque de implementación necesita resolver desafíos específicos, incluyendo la gestión de cambios a la cultura y el comportamiento.
COBIT 5 proporciona amplias y prácticas guías de implementación. Implementación, que está basada en un ciclo de vida de mejora continua. Orientado a ser una guía para evitar los obstáculos más comunes, aprovechar las mejores prácticas y ayudar en la creación de resultados

satisfactorios. La guía es complementada con una herramienta de implementación que contiene varios recursos que mejoraran continuamente. Sus contenidos incluyen:

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

Aspectos importantes de Implementación:

- Realizar un caso de negocio para la implementación y mejora del gobierno y gestión de TI.
- Reconocer los típicos puntos débiles y eventos desencadenantes.
- Crear el entorno apropiado para la implementación.
- Aprovechar COBIT para identificar carencias y guiar en el desarrollo de elementos facilitadores como políticas, procesos, principios, estructuras organizativas y roles y responsabilidades.
- Posicionamiento de GEIT en la organización.
- Adopción de los primeros pasos para mejorar GEIT.
- Factores de éxito y retos para la implementación.
- Habilitación del cambio de comportamiento y organizacional relacionado con el GEIT
- Uso de COBIT 5 y sus componentes.

FASES DE LA IMPLEMENTACION DEL CICLO DE VIDA

Atreves de la ilustración1-4 de las fases de implementación del ciclo de vida (ISACA, 2012) nos enseña un resumen de cada una de ellas.

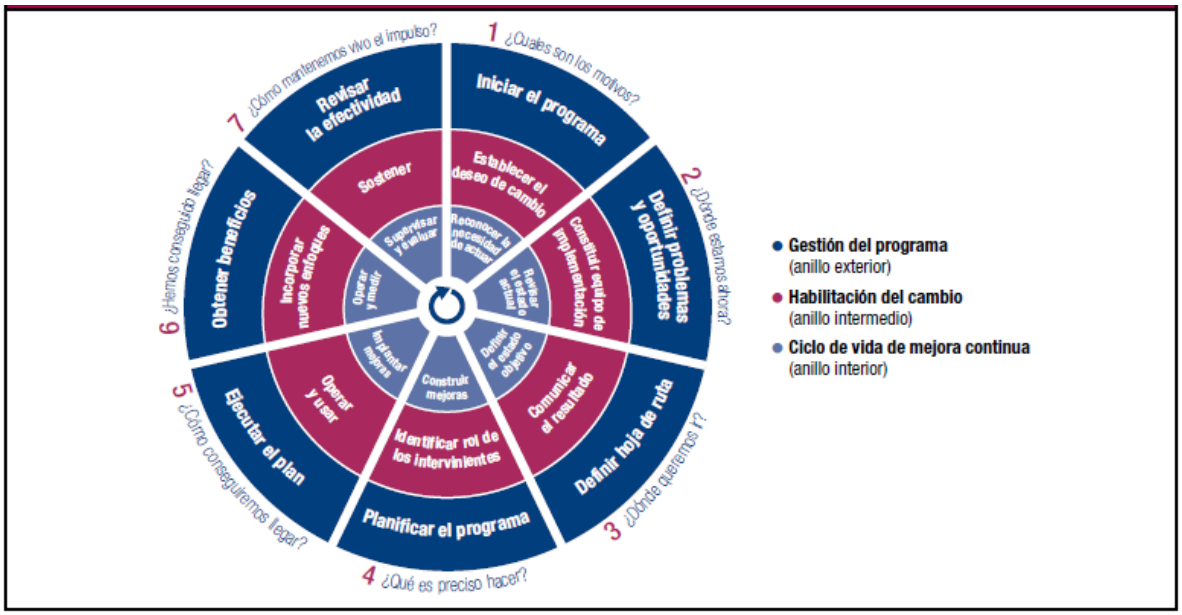


Ilustración 1-4Siete fases de la implementación del ciclo de vida (ISACA, 2012)

(ISACA, 2012) Señala en que consiste cada una de las fases:

La fase 1:

Reconocimiento y aceptación de la necesidad de una iniciativa de implementación o mejora.

Identificación de los puntos débiles actuales con los cuales desencadena y crea el ánimo de cambio.

La fase 2:

Define el alcance de la iniciativa de implementación o mejora empleando el mapeo de COBIT.

Considera a los escenarios de riesgos para destacar los procesos clave en los que focalizarse. Los diagnósticos de alto nivel nos ayudan a delimitar y entender áreas de alta prioridad.

Evalúa el estado actual e identifica los problemas y deficiencias mediante un proceso de revisión de capacidad.

Fase 3:

Establece un objetivo de mejora y análisis más detallado aprovechando las directrices de COBIT con el cual se identifican diferencias y posibles soluciones.

Fase 4:

La definición de proyectos permite planificar soluciones prácticas apoyadas.

Además, se desarrolla un plan de cambios para la implementación. Un caso de negocio desarrollado adecuadamente ayuda a asegurar que se identifican y supervisan los beneficios del proyecto.

Fase 5:

Las soluciones propuestas en la fase 4 son implementadas en prácticas en esta fase.

Fase 6:

Focaliza en la operación sostenible de los nuevos o mejorados catalizadores y de la supervisión de la consecución de los beneficios esperados.

Fase 7:

Revisa el éxito global de la iniciativa.

Identifican requisitos adicionales para el gobierno o la gestión de la TI empresarial

Refuerza la necesidad de mejora continua.

Modelo de capacidad de los procesos de COBIT 5

Vale recalcar que en COBIT 4.1 se conocía como modelo de madurez, en COBIT 5 se lo conoce como niveles de capacidad de procesos, en el cual podemos encontrar beneficios y diferencias que facilitan evaluar los procesos como se observa en la ilustración 1-5.

Nivel del Modelo de Madurez de Cobit 4.1	Capacidad del Proceso basada en ISO/IEC 15504	Contexto
5 Optimizado—Los procesos han sido refinados a nivel de buena práctica, sobre la base de los resultados de mejora continua y de modelado de madurez con otras empresas. Las TI se usan de forma integrada para automatizar los flujos de trabajo, proporcionando herramientas para mejorar la calidad y la efectividad, haciendo a la empresa rápida para adaptarse.	**Nivel 5: Proceso optimizado**—El proceso predecible del nivel 4 es mejorado continuamente para alcanzar metas de negocio actuales y futuros.	**Punto de Vista de la Empresa—Conocimiento Corporativo**
4 Gestionado y medible— Los responsables de la gestión monitorizan y miden el cumplimiento con procedimientos y llevan a cabo acciones donde los procesos parecen no estar funcionando con efectividad. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Automatización y herramientas son usadas de forma limitada o fragmentada.	**Nivel 4: Proceso establecido**—El proceso establecido del nivel 3 es operado ahora dentro de unos límites definidos para alcanzar sus resultados.	
3 Procesos definidos— Se han estandarizado, documentado y comunicado los procedimientos mediante formación. Es obligatorio seguir estos procedimientos, sin embargo es poco probable que se detecten desviaciones. Los procedimientos no son sofisticados en sí mismos, pero sí la formalización de las prácticas existentes.	**Nivel 3: Procesos establecidos**—El proceso gestionado del nivel 2 se implementa usando un proceso definido que es capaz de alcanzar sus objetivos.	
	Nivel 2: Proceso gestionado—El proceso ejecutado del nivel 1 es implementado de forma gestionada (planificado, supervisado y ajustado) y sus resultados son debidamente establecidos, controlados y mantenidos.	**Punto de Vista de la Instancia—Conocimiento Individual**
2 Repetible pero intuitivo— Los procesos están desarrollados hasta el punto que procedimientos similares son seguidos por personas diferentes ejecutando la misma tarea. No hay formación formal o comunicación de los procedimientos estándar, y la responsabilidad se deja a la persona de forma individual. Hay un alto grado de dependencia en el conocimiento individual y, por lo tanto, los errores son probables.	**Nivel 1: Proceso ejecutado**—El proceso implementado alcanza su objetivo. **Comentario: Es posible que algunos procesos clasificados como nivel 1 del Modelo de Madurez sean clasificados nivel 0 por ISO/IEC 15504 si los objetivos no son alcanzados.**	
1 Inicial/*Ad hoc*—Hay evidencia de que la empresa reconoce que existe el problema y que hay que abordarlo. Sin embargo, no hay procesos estandarizados. En su lugar hay enfoques *ad hoc* que tienden a aplicarse de forma individual o caso por caso. La aproximación general a la gestión es desorganizada.		
0 Inexistente—Ausencia completa de cualquier proceso reconocible. La empresa ni siquiera ha reconocido que hay un problema que gestionar.	**Nivel 0: Proceso incompleto**—El proceso no está implantado o no alcanza sus objetivos.	

Ilustración 1-5Comparación de los niveles de madurez (COBIT4.1) y los niveles de capacidad de proceso (COBIT5) (ISACA, 2012)

Para (ISACA, 2012)
COBIT 5 incluye un modelo de capacidad de procesos, basado en la norma internacionalmente reconocida ISO / IEC 15504 de Ingeniería de Software-Evaluación de Procesos. Este modelo alcanzará los mismos objetivos generales de evaluación de procesos y apoyo a la mejora de procesos, es decir, que proporcionará un medio para medir el desempeño de cualquiera de los procesos de gobierno (basado en EDM) o de gestión (basado en PBRM), y permitirá identificar áreas de mejora. (p. 41).

En este modelo de capacidad de procesos existen seis niveles de capacidad que definiré a continuación con la ayuda de (ISACA, 2012):

<u>Nivel 0.- Proceso incompleto:</u>

El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.

<u>Nivel 1 Proceso ejecutado:</u>

El proceso implementado alcanza su propósito.

Nivel 2 Proceso gestionado:

El proceso ejecutado descrito anteriormente está ya implementado de forma gestionada *(planificado, supervisado y ajustado)* y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.

Nivel 3 Proceso establecido:

El proceso gestionado descrito anteriormente está ahora implementado con el uso de un proceso definido que es capaz de alcanzar sus resultados de proceso.

Nivel 4 Proceso predecible:

El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.

Nivel 5 Proceso optimizado:

El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con las metas empresariales presentes y futuros.

Como resumen de los nivele definidos anteriormente tenemos la Ilustración 1-6:

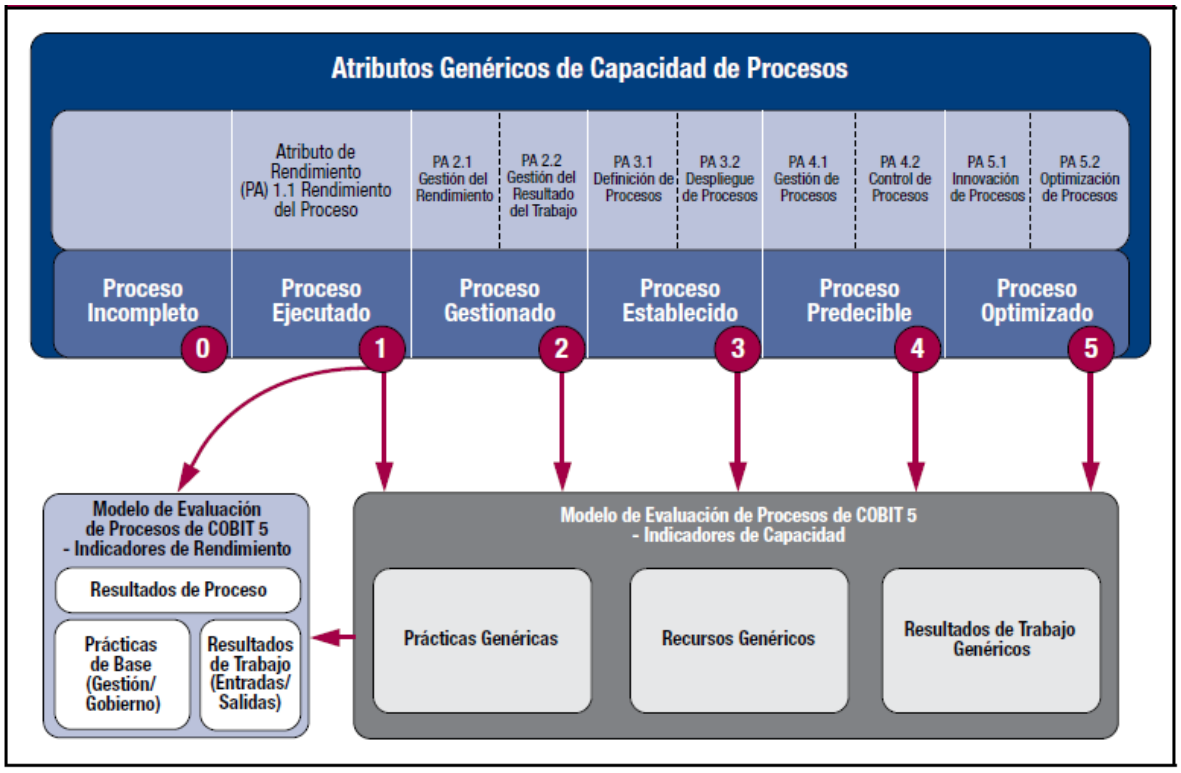


Ilustración 1-6Resumen del Modelo Capacidad de Procesos de COBIT 5 (ISACA, 2012)

CAPÍTULO 2

SITUACION ACTUAL DE LA UNIDAD EDUCATIVA "LA ASUNCION"

Seguridad de Redes COBIT como metodología

Con la elaboración de este capítulo lo que se busca es tener un amplio conocimiento sobre la Unidad Educativa "La Asunción"; describiéndola, conociendo quienes la conforman, su estructura orgánico- funcional e infraestructura *(inventarios, sistemas, diseños y esquemas)* relacionada área de sistemas, con la finalidad de ir sumando conocimientos para la elaboración de la Auditoría.

2.1 Descripción de la Unidad Educativa Particular "La Asunción"

Valores Institucionales

Ética: Honestidad en todas las acciones personales, sociales y profesionales.

Calidad: Responsabilidad con la formación integral de nuestros estudiantes, acorde con los estándares nacionales de calidad educativa.

Crecimiento y desarrollo: Coherencia entre el accionar y el enfoque humanístico en todo el proceso educativo institucional.

Aprendizaje e innovación: Responsabilidad con el desarrollo de aprendizajes orientados a la solución de problemas en forma innovadora y creativa.

Imagen corporativa: Alto sentido de identidad y percepción social de credibilidad y confianza institucional.

Cultura y clima organizacional: Actitud proactiva y creativa en la gestión institucional integral y en las relaciones interpersonales cotidianas.

Talento humano: Potenciación de las capacidades, habilidades y destrezas, para el logro de los objetivos institucionales.

Responsabilidad social: Respeto y compromiso consigo mismo, con los demás y con el entorno social y ambiental.

Diferenciación de servicios: Compromiso con la implementación de proyectos educativos acordes con las últimas tendencias pedagógicas, científicas y tecnológicas. (Unidad educativa "La Asunción", 2014-2015).

Ideario

- La educación que ofertamos contribuye a la construcción y transformación de nuestro país y reconoce a las niñas, niños y adolescentes como centro del proceso de aprendizaje.

- Impartimos una educación pluralista y garantizamos el interés superior de los niños, niñas y adolescentes.

- Promovemos en todos los espacios y momentos, la práctica constante de valores, como la libertad personal, la democracia, el respeto a los derechos, la responsabilidad, la solidaridad, la tolerancia, la honestidad, el respeto a la diversidad de género, étnica, social y creencia religiosa, y eliminamos toda forma de discriminación.

- Nuestra práctica educativa se sustenta en un enfoque de derechos, en un marco de libertad, dignidad, equidad social, cultural e igualdad de género.

- Valoramos el esfuerzo individual, motivamos a las personas para el aprendizaje y apoyamos la tarea docente como factor esencial de la calidad educativa.

- Fomentamos una cultura de paz y no violencia, a través del dialogo y las relaciones de buen trato y de afecto.

- Somos una institución educativa en constante búsqueda de la innovación, mediante el fomento de una cultura de investigación y el desarrollo del pensamiento crítico.

- Propiciamos una educación de calidad y calidez, mediante una forma contextualizada que responde a las necesidades del entorno social, natural y cultural; y la promoción de condiciones adecuadas de respeto, tolerancia y afecto, que generen un clima escolar favorable para el desarrollo de aprendizajes auténticos y flexibles.

- La formación se orienta al desarrollo de capacidades, de análisis y conciencia crítica para que las personas se inserten en la sociedad con vocación transformadora y de construcción de una sociedad justa, equitativa y libre.

- Brindamos una formación centrada en el educando para que desarrollaren la autonomía y el ejercicio gradual de sus libertades. (Unidad educativa “La Asunción”, 2014-2015).

Misión

Somos una Unidad Educativa Particular en mejora continua, conformada por profesionales en constante actualización, que brinda a niños y jóvenes un servicio educativo humanístico–integral,

acorde con las últimas tendencias pedagógicas, científicas y tecnológicas, en un ambiente de calidez, compromiso y responsabilidad social. (Unidad educativa “La Asunción”, 2014-2015)

Visión

Consolidarnos como Unidad Educativa de confianza y reconocimiento social, que se mantenga a la vanguardia de la educación, con propuestas pedagógicas innovadoras, ofreciendo una formación de seres humanos íntegros, que contribuyan a su transformación personal y del entorno social y ambiental. (Unidad educativa “La Asunción”, 2014-2015)

2.2 Estructura Orgánico-Funcional General

Número de docentes que laboran en la institución

La Unidad Educativa está conformada por:

Administrativos	29
Colegio	74
Escuela	66
Escuela de talentos	5 *(son compartidos con personal de la Escuela que laboran en la mañana o en la tarde o ambos).*
Mixto Psicólogo	1
Servicio	12

Jerarquía de los cargos ejercidos dentro de la institución.

JERARQUIA	DESCRIPCION
1	DIRECTOR DE LA UNIDAD EDUCATIVA DIRECTORA ESCUELA
2	SUBDIRECTORA DE LA ESCUELA VICERRECTOR
3	COORDINADORA DE DISCIPLINA INSPECTORA GENERAL
4	ADMINISTRADOR DE LA RED AUDIOVISUALES AUXILIAR ADMINISTRATIVO AUXILIAR DE COLECTURIA CONSERJE DIRECTORA DE PERSONAL DOCTORA ENFERMERA ENTRENADOR FINANCIERA

GUARDALMACEN
GUÍA DIRIGENTE
IMPRENTA
LABORATORISTA DE QUÍMICA
ORIENTADOR DEL DOBE COLEGIO
ORIENTADOR DEL DOBE ESCUELA
PROFESOR
PROGRAMADOR
RECEPCIONISTA
SECRETARIA GENERAL
SECRETARIA RECTORADO
TRABAJADORA SOCIAL

(Unidad educativa “La Asunción”, 2014-2015).

2.3 Directiva

Rector

Ing. Patricio Feijoo

Funciones

- Representar legalmente a la Unidad Educativa.
- Liderar la ejecución de la planeación estratégica institucional.
- Coordinar académica y administrativamente las labores de la Unidad Educativa “La Asunción”, con la Universidad del Azuay.
- Nombrar al personal docente, administrativo, personal de los laboratorios, talleres y de servicios generales, que hubieren triunfado en los concursos convocados para el efecto de acuerdo con las partidas del presupuesto particular.
- Establecer políticas, normas y objetivos institucionales, y aprobar los procedimientos para llevarlas a cabo.
- Disponer de un fondo rotativo equivalente a un 50% de un salario mínimo unificado, para gastos imprevistos requiera la institución.
- Participar como integrante del Consejo Ejecutivo de la Unidad Ejecutiva con voz y voto. (Unidad educativa “La Asunción”, 2014-2015).

Tareas

- Representar a la Unidad Educativa en asuntos Legales, académicos, sociales, culturales u otros a los que haya sido invitado o convocado, o delegar a un colaborador para que lo represente en los casos que sea pertinente.
- Participar y convocar a las instancias pertinentes para elaborar el plan estratégico institucional.
- Convocar a las instancias pertinentes para realizar las revisiones de la Dirección del plan estratégico institucional y para anualmente efectuar las modificaciones en caso de que fuera necesario.
- Establecer niveles, medios y espacios de comunicación para que esta sea efectiva y eficiente.

- Establecer la política salarial conjuntamente con el departamento financiero y departamento de personal.
- Aprobar todos los procedimientos, instructivos, u otros documentos que se generen para estandarizar la gestión de las diferentes instancias del plantel.
- Comprometerse con el proyecto educativo institucional vigente y brindar todo el respaldo a las instancias responsables de su implantación.
- Presentar a los organizamos de control correspondientes el proyecto educativo institucional y más documentos que se requieran.
- Integrar, motivar y comprender al personal directivo, docente, administrativo y de servicio, padres de familia y otros como aliados estratégicos de la ejecución del proyecto.
- Promover la elaboración de procedimientos y registros que lleven a la estandarización de actividades en las diferentes áreas docentes y administrativas.
- Aprobar el distributivo de trabajo de los colaboradores del plantel.
- Autorizar la inscripción de las matrículas de los estudiantes del colegio o de la Escuela, de acuerdo al cupo establecido dentro de las políticas institucionales. En ningún caso se sobrepasara el cupo señalado.
- Autorizar cambio de calificaciones por errores en la acreditación hecha por los docentes.
- Aprobar el horario general de clases, elaborado por la comisión nombrada para el efecto.
- Autorizar los gastos realizados por los fondos de caja chica y la reposición de los fondos.
- Coordinar con el Departamento Personal para realizar concursos para llenar vacantes de Personal Docente, Administrativo o de servicio, para organizar actividades de desarrollo personal o profesional del personal a su cargo.
- Coordinar con el Decanato General Administrativo de la Universidad del Azuay el uso de locales y espacios físicos comunes a los diversos niveles educativos.
- Mantener y fomentar buenas relaciones interpersonales en el Plantel. (Unidad educativa “La Asunción”, 2014-2015).

Vicerrector

Dr. María Patricia Arévalo Samaniego

Funciones

- Integrar el Consejo Ejecutivo de la Unidad Educativa
- Organizar la marcha académica del Colegio estableciendo directrices y objetivos educativos, acordes al PEI.
- Asesorar a los docentes en la planificación, ejecución y evaluación de los procesos enseñanzas aprendizaje.
- Realizar el seguimiento pedagógico a los docentes. (Unidad educativa “La Asunción”, 2014-2015).

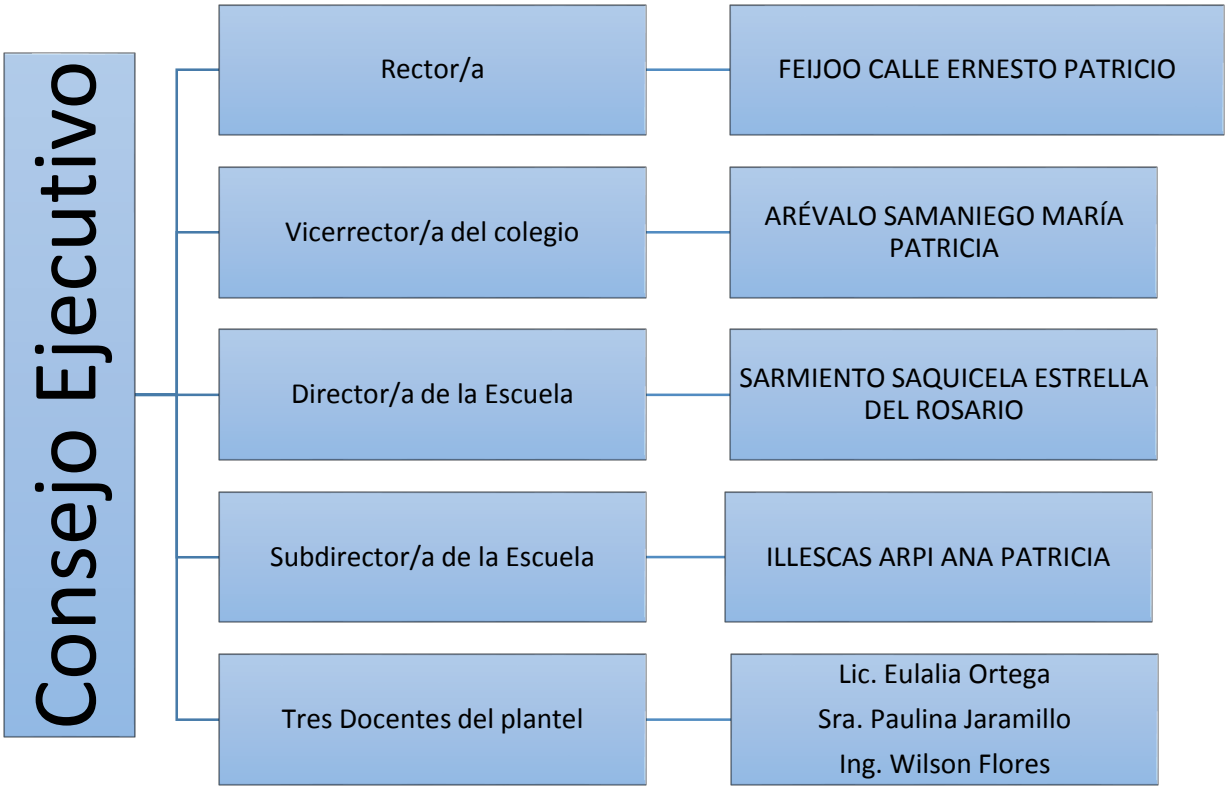
Tareas

- Elaborar el plan anual de actividades en coordinación con el/la directora(a) de la Unidad Educativa, Inspección General y la dirección de la Escuela.
- Presidir la Comisión Pedagógica, y las demás comisiones permanentes de la Institución.
- Determinar los lineamientos académicos que se tomaran en cuenta para el desarrollo de cada año lectivo y comunicar a los directores de área en la comisión pedagógica.
- Validar los materiales didácticos a ser utilizados en cada año lectivo en las diferentes áreas académicas y solicitar al/la director(a) de la Unidad Educativa su aprobación y adquisición.
- Revisar y aprobar los cuestionarios de exámenes quintrales, finales y supletorios, luego del informe favorable de/la directora(a) de área.
- Recibir, a los secretarios de las juntas de curso y de las comisiones permanentes, las actas debidamente legalizadas después de 48 horas de realizadas las sesiones, para el seguimiento y control de la ejecución de lo acordado.
- Organizar y controlar la entrega oportuna de los informes de aprovechamiento y disciplina del estudiantado, a sus representantes.
- Orientar y realizar el seguimiento de la elaboración y aplicación de los instrumentos de planificación didáctica y de los materiales utilizados, así como también de la evaluación de los aprendizajes a través de los informes presentados por los directores de área.
- Asesorar a los profesores del Colegio y directores de área en la elaboración de planes de mejora cuando se requiera.
- Participar periódicamente o cuando sea necesario, en las Juntas de Profesores de Área.
- Organizar y coordinar las juntas de curso.
- Responsabilizarse, en coordinación con el Rector, de la organización y ejecución de todos los actos internos y externos del Colegio y supervisar las actividades que lleven a cabo las distintas comisiones.
- Mantener reuniones permanentes con el/la Inspector/a General con el Objeto de analizar las acciones tendientes a mantener el orden y la disciplina en el Plantel.
- Conocer y encontrar soluciones, en coordinación con la Inspección y el Departamento de Orientación y Bienestar Estudiantil, para los problemas de orden académico y disciplinario entre los estudiantes y el profesorado.
- Responsabilizarse de la planificación, desarrollo pedagógico y evaluación de las actividades educativas en el Plantel, en coordinación con el Rectorado y demás Instancias académicas del Colegio.
- Supervisar y coordinar las actividades de comisión, actividades deportivas, sociales y extracurriculares.
- Establecer cronogramas para sesiones de trabajo con los diferentes organizamos del plantel.
- Orientar y supervisar el trabajo de la Comisión Especial de Evaluación Educativas y su coordinación con otras instancias del Plantel.
- Presidir y asesorar el Consejo de Orientación y Bienestar Estudiantil.
- Coordinar y orientar, junto con el profesor responsable, las actividades del Consejo Estudiantil para el cumplimiento de sus objetivos.

- Atender a los representantes de los estudiantes y al personal para solventar inquietudes sobre las actividades educativas, políticas, o problemas de comportamiento o de aprendizaje de los estudiantes.
- Participar en los procesos de selección de docentes para el Colegio.
- Mantener y fomentar buenas relaciones interpersonales en el Planeta.
- Entregar informes permanentes al/la directora/a de la Unidad Educativa sobre todas las actividades encomendadas. Presentar anualmente, al Consejo Directivo, el informe de las actividades efectuadas.
- Cumplir con otras actividades laborales temporales, encargadas por el Director de la Unidad Educativa. (Unidad educativa "La Asunción", 2014-2015).

Consejo Ejecutivo

El Consejo ejecutivo está jerárquicamente integrado por:



Funciones:

"Art. 50.- Consejo Ejecutivo.- Es la instancia directiva, de participación de la comunidad educativa y de orientación académica y administrativa de los establecimientos públicos, fiscomisionales y particulares.

El Consejo Ejecutivo está conformado por:

1. El Rector o Director, que lo preside y tiene voto dirimente;

2. El Vicerrector o Subdirector, según el caso, y,

3. Tres (3) vocales principales, elegidos por la Junta General de Directivos y Docentes y sus respectivos suplentes.

El Secretario del Consejo Ejecutivo debe ser el Secretario de la institución educativa. En caso de falta o ausencia de este, puede designarse un Secretario ad hoc. El Secretario tiene voz informativa, pero no voto.

El Consejo Ejecutivo se debe reunir ordinariamente por lo menos una (1) vez al mes, y extraordinariamente, cuando lo convoque el Rector o Director o a pedido de tres (3) de sus miembros. El Consejo Ejecutivo debe sesionar con la presencia de por lo menos la mitad más uno (1) de sus integrantes." (Ley Organica de educacion Superior, 2010).

2.4 Estructura Orgánico-Funcional Del Departamento de Sistemas

Misión:

La Unidad educativa no cuenta con misión por departamento.

Función:

El departamento de sistemas cuenta con dos principales funciones:

Administración de redes:

- Controlar y dar mantenimiento a los equipos como servidores y máquinas para usuarios finales.
- Administración de correo electrónico, pagina web, DNS, DHCP, internet, red inalámbrica.
- Soporte de hardware.
- Reparaciones.
- Mantenimiento correctivo y preventivo del hardware.

Desarrollo de software:

- Desarrollo de módulos según requerimiento.
- Reportería en base a necesidades.
- Soporte a usuarios en cuanto al manejo del sistema.

Unidades que la integran:

Ing. Jose Galarza.
Ing. Lorena Ruiz.

2.5 Infraestructura

Red Informática:

Se utiliza categoría 5 en infraestructura de red de datos de la Unidad Educativa.
Para la conexión del bloque B es decir del bloque o edificio que conforma el Colegio Particular "La Asunción" con la escuela se la realiza mediante fibra óptica; así mismo la interconexión con otros bloques existentes dentro de la Unidad Educativa también se la realiza mediante fibra óptica.
Se utiliza VLAN entre dependencias es decir, la VLAN es utilizada en el caso de los bloques que se encuentran aislados para toda dependencia.

Los switches que se utilizan son administrables dependiendo las necesidades de la Unidad Educativa.

El proveedor de Internet es la Universidad del Azuay, por lo tanto la Unidad Educativa "La Asunción" se acata a las políticas de seguridad que la Universidad les imponga. Toda la Unidad Educativa cuenta con conexión Wii-Fi.

2.5.1 Inventarios de Hardware y Software

Adjunto Anexo#1.xlsx

2.5.2 Sistemas en Red

Sistema académico

- Consulta de estudiantes o padres de familia.
- Calificaciones por parte de los docentes.

En el caso de las secretarias de la Unidad Educativa cuentan con un sistema propio para uso exclusivo de las mismas ya que en algunos casos por cualquier motivo el docente no entrego las calificaciones dentro de las fechas límites, las secretarias son las únicas que pueden hacer cambios pasadas las fechas límites bajo una solicitud que deberá ser aprobada previamente.

En el caso de trabajo social tiene acceso a la información de estudiantes para análisis de becas.

Sistema de planificaciones

Se tiene un programa para el ingreso de archivos de planificaciones por bloque, para que así los jefes de áreas puedan dar la aprobación de planificaciones y así finalmente pasar al vicerrectorado, el cual realiza la revisión final de los archivos de planificación.

Finalmente cuando están aprobado las planificaciones se puede subir las notas de los estudiantes.

Sistema de encuestas

El sistema de encuestas cuenta con encuesta a estudiantes (estudiantes vs docentes), docentes para gestión de calidad docentes vs jefes de área, servicios como buses, bares, etc. Para analizar la satisfacción en los servicios.

Sistema Estudiantado

Este sistema de estudiantado da acceso a la matriculación de estudiantes nuevos y estudiantes que pertenecen a la institución y en el caso de la escuela únicamente a primero de básica; todo esto se lo realiza desde junio hasta agosto vía web

Dentro del estudiantado se toma en cuenta tres áreas:

Primero de básica por destrezas.

Escuela y colegio por bloque cada quimestre está dividido en 5 bloques y son dos quimestres por año.

Dentro de la web también se cuenta con notificaciones de un estudiante o varios estudiantes a los padres de familia de forma general o forma individual.

Sistema de asistencia

Se registra la asistencia de estudiantes y personal en general.

Gestión de Trasporte

Se registra todos los estudiantes que utilizan trasporte.

Los docentes no tienen trasporte por parte de la institución.

Sistema de Evaluación

Evaluación de los tutores a guías de cursos.

Evaluación a bares.

Sistema médico a los estudiantes y personal

Ingreso y baja de medicación.

Historial médico de los pacientes.

Sistema De Gestión De Recursos Humanos

Lleva registro del personal, cargos, con sus respectivas fechas, información del personal ligada también con el departamento médico.

Sistema para tutoras del curso

En este sistema se registra la asistencia, calificaciones y notificación de los estudiantes.

Guías:

Tienen acceso a notificaciones, asistencia y calificaciones de los estudiantes.

2.5.3 Diseño de la red

Servidores UEA Ver en: Anexo#2.vsdx.

2.5.4 Esquema lógico de la red

Flujo de re de Datos Ver en: Anexo#3.vsdx.

Conclusión:

La elaboración de este capítulo ha permitido conocer el ambiente en el cual nos desenvolveremos, conociendo a la gente que lo rodea, la infraestructura y a obtener información que ayudará posteriormente a la Auditoría.

CAPÍTULO 3

PLAN DE AUDITORÍA PARA LA GESTIÓN DE RED

3.1 Alcance

El siguiente trabajo de Auditoría aplicará COBIT como metodología para la evaluación y análisis de los diferentes procesos y controles que se aplican en el área de la tecnología de la información.

La Auditoría se centrará en el análisis de la gestión de la seguridad informática que es aplicada actualmente en la red de datos de la Institución Educativa "La Asunción".

Ya que la Institución Educativa "La Asunción" está dedicada exclusivamente a la "mejora continua, conformada por profesionales en constante actualización, acorde con las últimas tendencias pedagógicas, científicas y tecnológicas, en un ambiente de calidez, compromiso y responsabilidad social". (Unidad educativa "La Asunción", 2014-2015). Para cumplir con la misión de la Institución, cada departamento debe rendir adecuadamente cada una de sus funciones dando lo mejor de sí, de aquí que se identifican aquellos que pertenecen al sistema de red ya nombrados en el capítulo 2 para mantenerse en operación constante.

Así, se parte del análisis donde se identificarán las debilidades existentes y sus riesgos potenciales, se expondrán una serie de conclusiones sobre los actuales procedimientos y controles de seguridad así como recomendaciones para el mejoramiento de la gestión de seguridad Informática.

3.2 Comunicado al Rectorado sobre el Inicio de Actividades

Ver: anexo#4.docx.

3.3 Procesos COBIT aplicables a la gestión de seguridad

La determinación de los procesos COBIT involucrados dentro de la gestión de seguridad en redes que permitirán llevar a cabo el desarrollo de la presente Auditoría, fue realizada siguiendo las recomendaciones de COBIT procesos habilitantes que fue publicado el 2012 por ISACA. Este documento expone los objetivos de control detallados de COBIT que tienen relación con la seguridad en un ambiente de T.I. Basándose en estos procesos, se ha seleccionado aquellos que tienen relación con la gestión de la seguridad de la red informática, y que sean aplicables a la Unidad Educativa La Asunción.

A continuación se exponen los objetivos de control por dominios que han sido escogidos para la ejecución del trabajo de Auditoría de la gestión de seguridad de la red informática.

ALINEAR PLANIFICAR Y ORGANIZAR

APO 01 Gestionar el marco de gestión de TI.
APO 07 Gestionar los recursos humanos.

APO 11 Gestionar la calidad.
APO 12 Gestionar el riesgo.
APO 13 Gestionar la Seguridad.

CONSTRUIR, ADQUIRIR E IMPLEMENTAR

BAI 02 Gestionar la definición de requisitos.
BAI 03 Gestionar la identificación y construcción de soluciones.

ENTREGA, SERVICIO Y SOPORTE

DSS 01 Gestionar operaciones.
DSS 02 Gestionar peticiones e incidentes de servicio.
DSS 04 Gestionar la continuidad.
DSS 05 Gestionar servicios de seguridad.

SUPERVISAR, ANALIZAR Y EVALUAR

MEA 03 Supervisar, evaluar y valorarla conformidad con los requerimientos externos.

3.3.1 Descripción general de los procesos COBIT5

APO01 Gestionar el Marco de Gestión de TI	**Área: Gestión** **Dominio: Alinear, Planificar y Organizar**
Descripción del Proceso Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.	
Declaración del Propósito del Proceso Proporcionar un enfoque de gestión consistente que permita cumplir los requisitos de gobierno corporativo e incluya procesos de gestión, estructuras, roles y responsabilidades organizativos, actividades fiables y reproducibles y habilidades y competencias.	

El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
01 Alineamiento de TI y estrategia de negocio	• Porcentaje de las metas y requerimientos estratégicos de la empresa soportados por las metas estratégicas para TI • Nivel de satisfacción de las partes interesadas con el alcance del portafolio de programas y servicios planeados • Porcentaje de los facilitadores de valor de TI mapeados con facilitadores de valor del negocio
02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	• Coste de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación • Número de problemas de no conformidad relativos a TI de los que se ha informado al consejo de administración o que han causado comentarios o bochorno públicos • Número de problemas de no conformidad con respecto a acuerdos contractuales con proveedores de servicios de TI • Cobertura de las evaluaciones de conformidad
09 Agilidad de las TI	• Nivel de satisfacción de los ejecutivos de la empresa con la capacidad de respuesta de TI a nuevos requerimientos • Número de procesos de negocio críticos soportados por infraestructuras y aplicaciones actualizadas • Tiempo medio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada
11 Optimización de activos, recursos y capacidades de las TI	• Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes • Tendencia de los resultados de las evaluaciones • Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades TI
15 Cumplimiento de las políticas internas por parte de las TI	• Número de incidentes relacionados con el incumplimiento de la política • Porcentaje de partes interesadas que comprenden las políticas • Porcentaje de políticas soportadas por estándares y prácticas de trabajo efectivas • Frecuencia de revisión y actualización de las políticas
16 Personal del negocio y de las TI competente y motivado	• Porcentaje del personal cuyas habilidades TI son suficientes para las competencias requeridas para su función • Porcentaje del personal satisfecho con su función TI • Número de horas de aprendizaje/prácticas por trabajador
17 Conocimiento, experiencia e iniciativas para la innovación de negocio	• Nivel de concienciación y comprensión de las posibilidades de innovación de TI del negocio ejecutivo. • Nivel de satisfacción de las partes interesadas con los niveles de experiencia e ideas de la innovación TI. • Número de iniciativas aprobadas resultantes de ideas innovadoras de TI.
Objetivos y Métricas de Procesos	
Meta del Proceso	**Métricas Relacionadas**
1. Se ha definido y se mantiene un conjunto eficaz de políticas.	• Porcentaje de políticas, estándares y otros elementos catalizadores activos documentados y actualizados • Fecha de las últimas actualizaciones del marco de trabajo y de los elementos catalizadores • Número de exposiciones a riesgos debidas a la inadecuación del diseño del entorno de control
2. Todos tienen conocimiento de las políticas y de cómo deberían implementarse.	• Número de empleados que asistieron a sesiones de formación o de sensibilización • Porcentaje de proveedores indirectos con contratos en los que se definen requisitos de control

Ilustración 3-001 APO 01 Gestionar el Marco de Gestión de TI.

(COBIT 5, 2012) PAG-51.

APO07 Gestionar los Recursos Humanos	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.	
Declaración del Propósito del Proceso Optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa.	

El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas:**
01 Alineamiento de TI y estrategia de negocio	• Porcentaje de las metas y requerimientos estratégicos de la empresa soportados por las metas estratégicas para TI • Nivel de satisfacción de las partes interesadas con el alcance del portafolio de programas y servicios planeados • Porcentaje de los facilitadores de valor de TI mapeados con facilitadores de valor del negocio
11 Optimización de activos, recursos y capacidades de las TI	• Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes • Tendencia de los resultados de las evaluaciones • Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades TI
13 Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	• Número de programas/proyectos ejecutados en plazo y en presupuesto • Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto • Número de programas que necesitan ser revisados significativamente debido a defectos de calidad • Coste del mantenimiento de aplicaciones respecto al coste total de TI
16 Personal del negocio y de las TI competente y motivado	• Porcentaje del personal cuyas habilidades TI son suficientes para las competencias requeridas para su función • Porcentaje del personal satisfecho con su función TI • Número de horas de aprendizaje/prácticas por trabajador
17 Conocimiento, experiencia e iniciativas para la innovación de negocio	• Nivel de sensibilización y comprensión de las posibilidades de innovación de TI por parte de los Ejecutivos de negocio • Nivel de satisfacción de las partes interesadas con los niveles de experiencia e ideas en innovación de las TI • Número de iniciativas aprobadas procedentes de ideas innovadoras de TI

Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. La estructura organizacional y las relaciones de TI son flexibles y dan respuesta ágil.	• Número de definiciones de servicio y catálogos de servicio •Nivel de satisfacción de los ejecutivos con la toma de decisiones de la gerencia • Número de decisiones que no pudieron resolverse dentro de las estructuras de gestión y se escalaron a las estructuras de gobierno
4. Los recursos humanos son gestionados eficaz y eficientemente.	• Porcentaje de rotación del personal • Duración media de las vacantes • Porcentaje de puestos de TI vacantes

Ilustración 3-2 APO 07 Gestionar los recursos humanos.

(COBIT 5, 2012) Pag-83.

APO11 Gestionar la Calidad	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.	
Declaración del Propósito del Proceso Asegurar la entrega consistente de soluciones y servicios que cumplan con los requisitos de la organización y que satisfagan las necesidades de las partes interesadas.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
05 Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI	• Porcentaje de inversiones de TI en los que la realización del beneficio se monitoriza a través del ciclo de vida económico completo. • Porcentaje de servicios TI en los que se realizan los beneficios esperados. • Porcentaje de las inversiones en TI donde los beneficios demandados son alcanzados o excedidos.
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	• Número de interrupciones del negocio debidas a incidentes en el servicio de TI • Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
13 Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	• Número de programas/proyectos ejecutados en plazo y en presupuesto • Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto • Número de programas que necesitan ser revisados significativamente debido a defectos de calidad • Coste del mantenimiento de aplicaciones respecto al coste total de TI
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Las partes interesadas están satisfechas con la calidad de los servicios y las soluciones.	• Promedio de satisfacción de las partes interesadas con las soluciones y servicios • Porcentaje de partes interesadas satisfechos con la calidad de TI • Número de servicios con un plan de gestión de la calidad formal
2. Los resultados de los proyectos y de los servicios entregados son predecibles.	• Porcentaje de proyectos revisados que cumplen con las metas y objetivos de calidad • Porcentaje de soluciones y servicios entregados con una certificación formal • Número de defectos sin descubrir antes de la puesta en producción
3. Los requisitos de calidad están implementados en todos los procesos.	• Número de procesos con un requisito de calidad definido • Número de procesos con un informe de evaluación formal de la calidad • Número de ANSs que incluyen criterios de aceptación de calidad

Ilustración 03-3 APO 11 Gestionar la calidad.

(COBIT 5, 2012) Pag-101.

APO12 Gestionar el Riesgo	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.	
Declaración del Propósito del Proceso Integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial general (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI.	
El proceso apoya la consecución de un conjunto de principales metas TI:	

El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
02 Cumplimiento y soporte de las TI al cumplimiento del negocio de las leyes y regulaciones externas	• Coste del incumplimiento de TI, incluyendo acuerdos judiciales y multas, y el impacto de pérdida de reputación • Número de asuntos de incumplimiento relacionados con TI reportados a la junta que llegan a ser de dominio público o que provocan situaciones de escándalo • Número de asuntos de incumplimiento relacionados con acuerdos contractuales con proveedores de servicio TI • Cobertura de la evaluación del cumplimiento
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo
06 Transparencia de los costes, beneficios y riesgo de las TI	• Porcentaje de inversión en casos de negocio con costes y beneficios esperados relativos a TI claramente definidos y aprobados. • Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados. • Encuesta de satisfacción a las partes interesadas clave relativa al nivel de transparencia, comprensión y precisión de la información financiera de TI.
10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública • Número de servicios de TI con los requisitos de seguridad pendientes • Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados • Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías
13 Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	• Número de programas/proyectos ejecutados en plazo y en presupuesto • Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto • Número de programas que necesitan ser revisados significativamente debido a defectos de calidad • Coste del mantenimiento de aplicaciones respecto al coste total de TI
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. El riesgo relacionado con TI está identificado, analizado, gestionado y reportado.	• Grado de visibilidad y reconocimiento en el entorno actual • Número de eventos de pérdida con características clave, capturados en repositorios • Porcentaje de auditorías, eventos y tendencias capturados en repositorios
2. Existe un perfil de riesgo actual y completo.	• Porcentaje de procesos de negocio claves incluidos en el perfil de riesgo • Completitud de atributos y valores en el perfil de riesgo
3. Todas las acciones de gestión para los riesgos significativos están gestionadas y bajo control.	• Porcentaje de propuestas de gestión de riesgos rechazadas debido a una falta de consideración sobre algún riesgo relacionado • Número de incidentes significativos no identificados e incluidos en el portafolio de gestión de riesgos
4. Las acciones de gestión de riesgos están efectivamente implementadas.	• Porcentaje de planes de acción para riesgos de TI ejecutados de la forma que fueron diseñados • Número de medidas que no reducen el riesgo residual

Ilustración 03-4 APO 12 Gestionar el riesgo.

(COBIT 5, 2012) Pag-107.

APO13 Gestionar la Seguridad	**Área: Gestión** **Dominio: Alinear, Planificar y Organizar**
Descripción del Proceso Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.	
Propósito Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.	

El proceso contribuye al logro de un conjunto de objetivos principales relacionados con TI:	
Metas TI	**Métricas Relacionadas**
02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	• Coste de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación • Número de problemas de no conformidad relativos a TI de los que se ha informado al consejo de administración o que han causado comentarios o bochorno públicos • Número de problemas de no conformidad con respecto a acuerdos contractuales con proveedores de servicios de TI • Cobertura de las evaluaciones de conformidad
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo
06 Transparencia de los costes, beneficios y riesgo de las TI	• Porcentaje de casos de inversión de negocio, que tienen claramente definidos y aprobados los costes y beneficios esperados relacionados con TI • Porcentaje de servicios de TI que tienen claramente definidos y aprobados los costes operacionales y los beneficios esperados • Encuestas de satisfacción dirigidas a los principales accionistas en relación al nivel de transparencia, entendimiento y precisión de la información financiera de TI
10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública • Número de servicios de TI con los requisitos de seguridad pendientes • Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados • Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías
14 Disponibilidad de información útil y relevante para la toma de decisiones	• Nivel de satisfacción de los usuarios del negocio y puntualidad (o disponibilidad) de la información de gestión • Número de incidentes en los procesos de negocio causados por la indisponibilidad de la información • Relación o cantidad de decisiones de negocio erróneas en las que la falta de información o la información errónea ha sido la principal causa

Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Está en marcha un sistema que considera y trata efectivamente los requerimientos de seguridad de la información de la empresa.	• Número de roles de seguridad claves claramente definidos •Número de incidentes relacionados con la seguridad
2. Se ha establecido, aceptado y comunicado por toda la empresa un plan de seguridad.	• Nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa • Número de soluciones de seguridad que se desvían del plan • Número de soluciones de seguridad que se desvían de la arquitectura de la empresa
3. Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en toda la empresa.	• Número de servicios con alineamiento confirmado al plan de seguridad • Número de incidentes de seguridad causados por la no observancia del plan de seguridad • Número de soluciones desarrolladas con alineamiento confirmado al plan de seguridad

Ilustración 03-5 Gestionar la seguridad.

(COBIT 5, 2012) Pag-113.

BAI02 Gestionar la Definición de Requisitos	Área: Gestión Dominio: Construir, Adquirir e Implementar
Descripción del Proceso Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costes y beneficios relacionados, análisis de riesgo y aprobación de los requerimientos y soluciones propuestas.	
Declaración del Propósito del Proceso Crear soluciones viables y óptimas que cumplan con las necesidades de la organización mientras minimizan el riesgo.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
01 Alineamiento de TI y estrategia de negocio	• Porcentaje de las metas y requerimientos estratégicos de la empresa soportados por las metas estratégicas para TI • Nivel de satisfacción de las partes interesadas con el alcance del portafolio de programas y servicios planeados • Porcentaje de los facilitadores de valor de TI mapeados con facilitadores de valor del negocio
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	• Número de interrupciones del negocio debidas a incidentes en el servicio de TI • Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
12 Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	• Número de incidentes en los procesos de negocio debidos a errores de integración tecnológica • Número de cambios en los procesos de negocio que necesitan ser retrasados o modificados debido a problemas de integración tecnológica. • Número de procesos de negocio habilitados por TI que se retrasan o incurren en un mayor coste debido a asuntos de integración tecnológica • Número de aplicaciones o infraestructuras críticas operando en silos sin integración
Objetivos y Métricas del Proceso	
Objetivos del Proceso	**Métricas Relacionadas**
1. Los requerimientos funcionales y técnicos del negocio reflejan las necesidades y expectativas de la organización.	• Porcentaje de requerimientos repetidos debido a la no alineación entre las necesidades y expectativas de la organización • Nivel de satisfacción de las partes interesadas con los requerimientos
2. La solución propuesta satisface los requerimientos funcionales, técnicos y de cumplimiento del negocio.	• Porcentaje de requerimientos satisfechos por la solución propuesta
3. El riesgo asociado con los requerimientos ha sido tomado en cuenta en la solución propuesta.	• Números de incidentes no identificados como riesgo • Porcentaje de riesgos no mitigado exitosamente
4. Los requerimientos y soluciones propuestas cumplen con los objetivos del caso de negocio (valor esperado y costes probables).	• Porcentaje de los objetivos del caso de negocio alcanzados por la solución propuesta • Porcentaje de partes interesadas que no aprueban la solución con relación al caso de negocio

Ilustración 03-6 BAI 02 Gestionar la definición de requisitos.

(COBIT 5, 2012) Pag-129.

BAI03 Gestionar la Identificación y Construcción de Soluciones	Área: Gestión Dominio: Construir, Adquirir e Implementar
Descripción del Proceso Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.	
Declaración del Propósito del Proceso Establecer soluciones puntuales y rentables capaces de soportar la estrategia de negocio y objetivos operacionales.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	• Número de interrupciones del negocio debidas a incidentes en el servicio de TI • Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. El diseño de la solución, incluyendo los componentes relevantes, debe cumplir con las necesidades de la empresa, alineándose con estándares y tratando todos los riesgos identificados.	• Número de rediseños realizados debido a discordancias con los requerimientos • Tiempo para aprobar que el entregable de diseño ha cumplido los requerimientos
2. La solución conforme al diseño, es acorde a las normas organizativas y cuenta con controles, seguridad y 'auditabilidad' apropiadas.	• Número de excepciones al diseño observadas durante la fase de revisión
3. La solución es de una calidad aceptable y ha sido probada convenientemente.	• Número de errores encontrados durante las pruebas • Tiempo y esfuerzo para completar las pruebas
4. Los cambios aprobados de los requerimientos están correctamente incorporadas a la solución.	• Número de cambios aprobados y registrados que generan nuevos errores
5. Las actividades de mantenimiento cumplen satisfactoriamente con las necesidades tecnológicas y de negocio.	• Número de solicitudes de mantenimiento no atendidas

Ilustración 03-7 BAI03 Gestionar la Identificación y Construcción de Soluciones.

(COBIT 5, 2012) Pag-133.

DSS01 Gestionar Operaciones	Área: Gestión Dominio: Entrega, Servicio y Soporte
Descripción del Proceso Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.	
Declaración del Propósito del Proceso Entregar los resultados del servicio operativo de TI, según lo planificado.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	• Número de interrupciones del negocio debidas a incidentes en el servicio de TI • Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
11 Optimización de activos recursos y capacidades de TI	• Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes • Tendencia de los resultados de las evaluaciones • Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades TI
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Las actividades operativas se realizan según lo requerido y programado.	• Número de procedimientos operativos no estándar ejecutados • Número de incidentes causados por problemas operativos
2. Las operaciones son monitorizadas, medidas, reportadas y remediadas.	• Tasa de eventos comparada con el número de incidentes • Porcentaje de tipos de eventos operativos críticos cubiertos por sistemas de detección automática

Ilustración 03-8 DSS 01 Gestionar Operaciones.

(COBIT 5, 2012) Pag-173.

DSS02 Gestionar Peticiones e Incidentes de Servicio	Área: Gestión Dominio: Entrega, Servicio y Soporte
Descripción del Proceso Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.	
Declaración del Propósito del Proceso Lograr una mayor productividad y minimizar las interrupciones mediante la rápida resolución de consultas de usuario e incidentes.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	• Número de interrupciones del negocio debidas a incidentes en el servicio de TI • Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
Objetivos y Métricas del Proceso	
Objetivos del Proceso	**Métricas Relacionadas**
1. Los servicios relacionados con TI están disponibles para ser utilizados.	• Número y porcentaje de incidentes que causan interrupción en los procesos críticos de negocio • Tiempo promedio entre incidentes de acuerdo con el servicio facilitado por TI
2. Los incidentes son resueltos según los niveles de servicio acordados.	• Porcentaje de incidentes resueltos dentro de un periodo acordado/ aceptable
3. Las peticiones de servicio son resueltas según los niveles de servicio acordados y la satisfacción del usuario.	• Nivel de satisfacción del usuario con la resolución de las peticiones de servicio • Tiempo promedio transcurrido para el tratamiento de cada tipo de petición de servicio

Ilustración 03-9 DSS 02 Gestionar Peticiones e Incidentes de Servicio.

(COBIT 5, 2012) Pag-177.

DSS04 Gestionar la Continuidad	Área: Gestión Dominio: Entrega, Servicio y Soporte
Descripción del Proceso Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.	
Declaración del Propósito del Proceso Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo
07 Entrega de servicios TI de acuerdo a los requisitos del negocio	• Número de interrupciones del negocio debidas a incidentes en el servicio de TI • Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
14 Disponibilidad de información útil y relevante para la toma de decisiones	• Nivel de satisfacción de los usuarios del negocio y puntualidad (o disponibilidad) de la información de gestión • Número de incidentes en los procesos de negocio causados por la indisponibilidad de la información • Relación o cantidad de decisiones de negocio erróneas en las que la falta de información o la información errónea ha sido la principal causa
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. La información crítica para el negocio está disponible para el negocio en línea con los niveles de servicio mínimos requeridos.	• Porcentaje de servicios TI que cumplen los requisitos de tiempos de funcionamiento • Porcentaje de restauraciones satisfactorias y en tiempo de copias alternativas o de respaldo • Porcentaje de medios de respaldo transferidos y almacenados de forma segura
2. Los servicios críticos tienen suficiente resiliencia.	• Número de sistemas críticos para el negocio no cubiertos por el plan
3. Las pruebas de continuidad del servicio han verificado la efectividad del plan.	• Número de ejercicios y pruebas que han conseguido los objetivos de recuperación • Frecuencia de las pruebas
4. Un plan de continuidad actualizado refleja los requisitos de negocio actuales.	• Porcentaje de mejoras acordadas que han sido reflejadas en el plan • Porcentaje de asuntos identificados que se han incluido satisfactoriamente en el plan
5. Las partes interesadas internas y externas han sido formadas en el plan de continuidad.	• Porcentaje de interesados internos y externos que han recibido formación • Porcentaje de asuntos identificados que se han tratado subsecuentemente en los materiales de formación

Ilustración 3-10 DSS 04 Gestionar la Continuidad.

(COBIT 5, 2012) Pag-185.

DSS05 Gestionar Servicios de Seguridad	Área: Gestión Dominio: Entrega, Servicio y Soporte
Descripción del Proceso Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.	
Declaración del Propósito del Proceso Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	• Coste de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación • Número de problemas de no conformidad relativos a TI de los que se ha informado al consejo de administración o que han causado comentarios o bochorno públicos • Número de problemas de no conformidad con respecto a acuerdos contractuales con proveedores de servicios de TI • Cobertura de las evaluaciones de conformidad
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo
10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública • Número de servicios de TI con los requisitos de seguridad pendientes • Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados • Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. La seguridad de las redes y las comunicaciones cumple con las necesidades del negocio.	• Número de vulnerabilidades descubiertas • Número de rupturas (*breaches*) de cortafuegos
2. La información procesada, almacenada y transmitida en los dispositivos de usuario final está protegida.	• Porcentaje de individuos que reciben formación de concienciación relativa al uso de dispositivos de usuario final • Número de incidentes que impliquen dispositivos de usuario final • Número de dispositivos de usuario final no autorizados detectados en la red o en el entorno
3. Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en el negocio.	• Promedio de tiempo entre los cambios y actualizaciones de cuentas • Número de cuentas (con respecto al número de usuarios/empleados autorizados)
4. Se han implantado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida.	• Porcentaje de pruebas periódicas de los dispositivos de seguridad del entorno • Clasificación media para las evaluaciones de seguridad física • Número de incidentes relacionados con seguridad física
5. La información electrónica tiene las medidas de seguridad apropiadas mientras está almacenada, transmitida o destruida.	• Número de incidentes relacionados con accesos no autorizados a la información

Ilustración 3-11 DSS 05 Gestionar Servicios de Seguridad.

(COBIT 5, 2012) Pag-191.

MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Área: Gestión Dominio: Supervisar. Evaluar y Valorar
Descripción del Proceso Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general.	
Declaración del Propósito del Proceso Asegurar que la empresa cumple con todos los requisitos externos que le sean aplicables.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	• Coste de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación • Número de problemas de no conformidad relativos a TI de los que se ha informado al consejo de administración o que han causado comentarios o bochorno públicos • Número de problemas de no conformidad con respecto a acuerdos contractuales con proveedores de servicios de TI • Cobertura de las evaluaciones de conformidad
04 Riesgos del negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo
Objetivos y Métricas del proceso	
Meta del Proceso	**Métricas Relacionadas**
1. La totalidad de los requisitos externos de cumplimiento se han identificado.	• Tiempo medio transcurrido entre la identificación de los problemas de incumplimiento y su resolución • Frecuencia de revisiones de cumplimiento.
2. Tratar adecuadamente los requisitos externos de cumplimiento.	• Número anual de incidentes críticos por incumplimiento • Porcentaje de propietarios de procesos que hayan confirmado por escrito el cumplimiento de requisitos externos

Ilustración 03-12 MEA 03 Supervisar, evaluar y valorar la conformidad con los requerimientos externos.

(COBIT 5, 2012) Pag. 213.

Alinear, Planificar y Organizar (APO)

APO 01 Gestionar el marco de gestión de TI

Ayuda a conocer si las responsabilidades de seguridad están definidas, entendidas y asignadas apropiadamente.

Los objetivos de control considerados son:

APO01.02 Establecer roles y responsabilidades.

APO07 Gestionar los Recursos Humanos

Con la finalidad de asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y sean conscientes de los riesgos y responsabilidades involucrados.

Los objetivos de control considerados son:

APO07.03 Mantener las habilidades y competencias del personal.

APO11 Gestionar la Calidad

Es necesario identificar que es necesario para cumplir con las obligaciones de seguridad con respecto a la privacidad, derechos de propiedad intelectual y otras regulaciones legales al existir requerimientos externos.

Los objetivos de control considerados son:

APO11.03 Enfocar la gestión de la calidad en los clientes.

APO11.06 Mantener una mejora continua.

APO12 Gestionar el Riesgo

Permite identificar problemas con la seguridad de TI y su impacto en los objetivos del negocio, además de considerar la manera de asegurar datos y transacciones que son críticos para el negocio, preparar un plan de acción para manejo de riesgos y concientizar al personal sobre los riesgos de seguridad.

Los objetivos de control considerados son:

APO12.01 Recopilar datos.

APO12.03 Mantener un perfil de riesgo.

APO12.06 Responder al riesgo.

APO13 Gestionar la Seguridad

Todo lo respecto a seguridad, contempla el control de acceso a sistemas para los diferentes usuarios, detectar, reportar y solucionar incidentes de violación de seguridad.

Los objetivos de control considerados son:

APO13.01 Establecer y mantener un SGSI.

APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.

APO13.03 Supervisar y revisar el SGSI.

Construir, Adquirir e Implementar (BAI)

BAI02 Gestionar la Definición de Requisitos

Se refiere a la seguridad apropiada para la infraestructura tecnológica (hardware y software) que tiene que ver con la actualización, mantenimiento y adquisición.

Los objetivos de control considerados son:

BAI02.03 Gestionar los riesgos de los requerimientos.

BAI03 Gestionar la Identificación y Construcción de Soluciones

Igual que el anterior proceso se refiere a la seguridad apropiada para la infraestructura tecnológica (hardware y software) que tiene que ver con la actualización, mantenimiento y adquisición.

Los objetivos de control considerados son:

BAI03.03 Desarrollar los componentes de la solución.

BAI03.10 Mantener soluciones.

Entrega, Servicio y Soporte (DSS)

DSS01 Gestionar Operaciones
Hace referencia a la seguridades físicas del área de Tecnología de Información incluye cableado de red, equipos de comunicación, computadores, periféricos y electricidad.

Los objetivos de control considerados son:

DSS01.04 Gestionar el entorno.
DSS01.05 Gestionar las instalaciones.

DSS02 Gestionar Peticiones e Incidentes de Servicio
Contempla el control de acceso a sistemas para los diferentes usuarios, detectar, reportar y solucionar incidentes de violación de seguridad, protección de respaldos, etc.

Los objetivos de control considerados son:

DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.

DSS04 Gestionar la Continuidad
Se refiere a la capacidad de la empresa de seguir brindando el servicio contando con un plan de contingencias para la recuperación de fallas después de incidentes en un tiempo mínimo y disponer de respaldos confiables.

Los objetivos de control considerados son:

DSS04.04 Ejercitar, probar y revisar el plan de continuidad.
DSS04.06 Proporcionar formación en el plan de continuidad.
DSS04.07 Gestionar acuerdos de respaldo.

DSS05 Gestionar Servicios de Seguridad
Comprende seguridades físicas del área de Tecnología de Información y control de acceso a sistemas para los diferentes usuarios y constancia en la seguridad de la información.

Los objetivos de control considerados son:

DSS05.01 Proteger contra software malicioso (malware).
DSS05.02 Gestionar la seguridad de la red y las conexiones.
DSS05.03 Gestionar la seguridad de los puestos de usuario final.
DSS05.04 Gestionar la identidad del usuario y el acceso lógico.
DSS05.05 Gestionar el acceso físico a los activos de TI.
DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.

Supervisar, Evaluar y Valorar (MEA)

MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.
Evaluar el cumplimiento de requisitos regulatorios y contractuales en los procesos de TI.

Los objetivos de control considerados son:

MEA03.01Identificar Requisitos externos de cumplimiento.

3.4 Herramientas útiles para el desarrollo de la Auditoría

Para poner en práctica el procedimiento de Auditoría se gestionará la recolección de datos y documentación necesaria, además se tomarán como guías los siguientes documentos:

COBIT 5 Enabling Processes *(Procesos Catalizadores).*
COBIT 5 Un marco de negocio para el Gobierno y la Gestión de las TI de la Empresa.

3.5 Plan de Auditoría

A continuación se presentan las principales actividades para realizar este trabajo de Auditoría:

1. Descripción de la Organización Administrativa:
   - Infraestructura Actual de la Red.
     Se hace uso de lo adquirido en el capítulo anterior el flujo de red de datos y servidores actualizados.
   - Evaluación de Riesgos de la Gestión de Seguridad de la Red Informática.
     La evaluación de riesgos se lo realiza con la información proporcionada y en base a la siguiente matriz:

MATRIZ DE EVALUACIÓN DE RIESGOS							
RECURSOS	AMENAZA	VULNERABILIDAD	CONTROL EXISTENTE	IMPACTO	PROBABILIDAD	NIVEL DE RIESGO	RECOMENDACIONES

2. Elaboración del Plan de Auditoría:
   - Definición del alcance de la Auditoría.
     Se define que alcance tendrá el proceso a realizarse durante la Auditoría.
   - Proceso en el dominio de supervisar, evaluar y valorar.
     Respecto a este proceso se toma en consideración los objetivos de control aplicables a esta Auditoría.
3. Puesta en marcha del Plan de Auditoría:
   - Elaboración del Programa de Auditoría.
     El programa de Auditoría se realizará en base a la siguiente matriz:

DOMINIO: ----------	
Nombre del Dominio	
Definicion del Dominio	
Objetivo de Control Detallado	Factores de Riesgo

- Elaboración de Matriz de Pruebas.
  Se lo realizará en base a la siguiente matriz:

Nombre del Dominio		
Objetivo de Control Detallado	**Revisión a través de:**	**Descripción de la Prueba**
	Evaluación de Controles: xxxxxxxxxxxxxxxxxx Probando que: xxxxxxxxxxxxxxxxxxx	

- Recolección de documentación: manuales de procedimientos, funciones y políticas.

4. Evaluación y Análisis de las pruebas realizadas
   La evaluación de resultados se realizará con la siguiente matriz:

DOMINIO: Supervisar, evaluar y valorar				
MEA 03. Supervisar, evaluar y valorar la conformidad con los requerimientos externos				
MEA 03.01. Identificar requisitos externos de cumplimiento.				
Revisión a través de:	**Descripción de la Prueba**	**Evaluación**	**Documentos de Soporte**	**Recomendación**
Evaluación de controles: xxxxxxxxxxxxxxxx Probando que: xxxxxxxxxxxxxxxx				

En base al análisis de pruebas efectuado se podrá determinar si los objetivos de control cumplen o no con las condiciones necesarias para su efectivo desempeño.

5. Elaboración del Informe Preliminar
   El Informe preliminar estar compuesto por:
   - Alcance de la Auditoría.
   - Objetivos de la Auditoría.
   - Temas considerados críticos.

- Cada tema estará compuesto por:
  Observación.
  Recomendaciones.
  Resultado de la discusión con el Gerente de TI.

6. Elaboración del Informe Final:

El informe final estará compuesto por una carta dirigida al rector de la Unidad Educativa La Asunción en la cual detallará lo siguiente:

- Fecha de inicio de la Auditoría.
- Fecha de redacción de informe de Auditoría.
- Encargados de la Auditoría.
- Alcance de Auditoría
- Objetivos de la Auditoría
- Objetivos de control considerados críticos
  - En cada objetivo se detallará lo siguiente:
    Observación.
    Riesgo.
    Recomendación.

Conclusión:

La elaboración de este capítulo fue muy importante para realizar la planificación de Auditoría con la finalidad de tener claro el panorama al momento de ejecutar la Auditoría. Se cuenta con fechas tentativas y un modelo de matrices que ayudarán a evaluar la Auditoría efectuada. Se ha procedido además a comunicar al Rector de la Unidad educativa "La Asunción" el inicio de actividades, recalcando la importancia de este paso en un proceso de Auditoría, con la finalidad de que él Rector de aviso a todo el personal y colabore con el mismo.

CAPÍTULO 4

PUESTA EN MARCHA DEL PLAN DE AUDITORÍA PARA LA GESTIÓN DE RED

4.1 Procesos en el dominio supervisar, evaluar y valorar

El desarrollo del Plan de Auditoría se enfocará en la elaboración del programa de Auditoría para el proceso de supervisar, evaluar y valorar, en el objetivo de control detallado (MEA03.01) en el cual se determinará los factores de riesgo aplicados al objetivo en cuestión.

A partir de éste y tomando como base las Directrices de Auditoría COBIT se desarrollará la matriz de pruebas en la cual se definirán las pruebas específicas a ser aplicadas para determinar el cumplimiento del objetivo de control detallado.

4.1.1 Evaluación de Riesgos de la Gestión de Seguridad de la Red Informática

A continuación se señalará los riesgos encontradas dentro de la red informática basándonos en el análisis del diseño de red y en el esquema lógico de la red proporcionada por la unidad educativa; y en la información proporcionada por el departamento de Sistemas.

Cuadro 4.1.1.1 Matriz de evaluación de riesgos.

MATRIZ DE EVALUACIÓN DE RIESGOS

RECURSOS	AMENAZA	OBSERVACIONES	CONTROL EXISTENTE	IMPACTO	PROBABILIDAD	NIVEL DE RIESGO	RECOMENDACIÓNES
Servidores y Pc	Mal uso de recursos no existe documentos de políticas	No existe documento de políticas de TI, no cuenta con un proceso de revisión definido	Ninguno	Alto	Alto	Alto	Crear una documentación de procedimientos que sea actualizada periódicamente
Servidores y Pc	Existe restricciones a información confidencial pero no existe un documento de políticas de confidencialidad	No existe documento de procedimientos de TI, no cuenta con un proceso de revisión definido	Ninguno	Media	Media	Alto	Crear una documentación de procedimientos que sea actualizada periódicamente
Equipos de conexión de red	Mal uso de recursos no existe documentos de políticas	No existe documento de procesos de TI, no cuenta con un proceso de revisión definido	Ninguno	Alto	Alto	Alto	Crear una documentación de procedimientos que sea actualizada periódicamente
Servidores y Pc	Existe restricciones a información confidencial pero no existe un documento de políticas de confidencialidad	No cuentan con documento de políticas de seguridad de TI	Ninguno	Alto	Alto	Alto	Crear una documentación de políticas de seguridad de TI que sea actualizada periódicamente

Cuadro 4.1.1.1 Matriz de evaluación de riesgos.

MATRIZ DE EVALUACIÓN DE RIESGOS

RECURSOS	AMENAZA	OBSERVACIONES	CONTROL EXISTENTE	IMPACTO	PROBABILIDAD	NIVEL DE RIESGO	RECOMENDACIÓNES
Equipos de conexión de red	Mal Uso de recursos	No existe un documento especifico de políticas de seguridad de TI	Ninguno	Alto	Alto	Alto	Crear una documentación de políticas de seguridad de TI que sea actualizada periódicamente
Aplicaciones en red (Sistema de Gestión Académica Web)	Acceso no autorizado a información confidencial	La aplicación dentro de la base de datos no guarda confidencialidad de sus cuentas y contraseñas	Los responsables de la base de datos conocen su responsabilidad sobre la divulgación de las cuentas	Alto	Medio	Medio	Cifrar las claves de los usuarios del sistema de gestión académica
Aplicaciones en red (Sistema de Gestión Académica De Escritorio)	Acceso no autorizado a información confidencial	La aplicación dentro de la base de datos no guarda confidencialidad de sus cuentas y contraseñas	Los responsables de la base de datos conocen su responsabilidad sobre la divulgación de las cuentas	Alto	Medio	Medio	Cifrar las claves de los usuarios del sistema de gestión académica

Cuadro 4.1.1.1 Matriz de evaluación de riesgos.

MATRIZ DE EVALUACIÓN DE RIESGOS

RECURSOS	AMENAZA	OBSERVACIONES	CONTROL EXISTENTE	IMPACTO	PROBABILIDAD	NIVEL DE RIESGO	RECOMENDACIÓNES
Aplicaciones en red (Sistema de Gestión Académica Web)	Ingreso de datos erróneos que produzcan mal información y no confiable	Existe la posibilidad de ingresar mal información en los campos ya que no están validados.	El administrador de red recibe un mail de mal ingreso de la información	Alto	Bajo	Alto	Crear validación para todos los campos, con la finalidad de que no se de aviso solo al administrador de red sino también al usuario
Aplicaciones en red (Sistema de Gestión Académica De Escritorio)	Ingreso de datos erróneos que produzcan mal información y no confiable	Existe la posibilidad de ingresar mal información en los campos ya que no están validados.	El administrador de red recibe un mail de mal ingreso de la información	Alto	Bajo	Alto	Crear validación para todos los campos, con la finalidad de que no se de aviso solo al administrador de red sino también al usuario

4.1.2 Elaboración del Plan de Auditoría

4.1.2.1. Definición del Alcance de Auditoría

La Auditoría se llevará a cabo en el domino de "supervisa, evaluar y valorar", en el objetivo de control de "Identificar requisitos externos de cumplimiento"; el alcance que tendrá este proceso es: definir los registros de requisitos de cumplimiento, inventario de acciones de cumplimiento necesarias, se identificarán las debilidades existentes y sus riesgos potenciales, se expondrán una serie de conclusiones sobre el procedimiento y controles de seguridad así como recomendaciones para el mejoramiento de la gestión de seguridad Informática.

4.1.2.2. Proceso en el dominio de supervisar, evaluar y valorar

El Objetivo de control detallado a ser considerado es:
"MEA 03.01 Identificar requisitos externos de cumplimiento".

Cuadro 4.1.2.2.1 Matriz de asignación de responsabilidades (RACI).

Matriz RACI MEA03																										
Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
MEA03.01 Identificar requisitos externos de cumplimiento.					A	R										R	R	R								R

Ilustración 04-1Matriz RACI.

(COBIT 5, 2012) Pag. 213.

4.2.1 Puesta en marcha del plan de Auditoría

Cuadro 4.2.1.1 Programa de Auditoría MEA03.01.

DOMINIO: Supervisar, evaluar y valorar.	
MEA03. Supervisar, evaluar y valorar la conformidad con los Requerimientos Externos.	
Asegurar que la empresa cumple con todos los requisitos externos que sean aplicables.	
Objetivo de Control Detallado	**Factores de Riesgo**
MEA 03.01 Identificar requisitos externos de cumplimiento "Identificar y supervisar, de manera continuada, cambios en las legislaciones y regulaciones tanto locales como internacionales, así como otros requisitos externos de obligado cumplimiento en el área de TI." (COBIT 5, 2012) Pag. 214 **Actividades** • Asignar la responsabilidad de identificar y supervisar los cambios legales y regulatorios y otros requisitos contractuales externos aplicables a la utilización de recursos de TI y al procesamiento de la información dentro de las operaciones de negocio y de TI (COBIT 5, 2012) Pag. 214 • Identificar y valorar la totalidad de los posibles requisitos de cumplimiento y su impacto sobre las actividades de TI en ámbitos como los flujos de datos, la privacidad, los controles internos, los informes financieros, la regulación sectorial, la propiedad intelectual y la seguridad en el trabajo. (COBIT 5, 2012) Pag. 214 • Mantener un inventario actualizado de los requisitos legales, regulatorios y contractuales aplicables, su impacto y las acciones	No haber definido los requisitos externos que rigen a la institución. Uso desleal de las legislaciones y regulaciones Incumplimiento de las legislaciones y regulaciones

DOMINIO: Supervisar, evaluar y valorar.	
MEA03. Supervisar, evaluar y valorar la conformidad con los Requerimientos Externos.	
Asegurar que la empresa cumple con todos los requisitos externos que sean aplicables.	
Objetivo de Control Detallado	**Factores de Riesgo**
necesarias. (COBIT 5, 2012) Pag. 214 • Mantener un registro general consolidado de los requisitos externos de cumplimiento que afecten a la empresa. (COBIT 5, 2012) Pag. 214	

Cuadro 4.2.1.2 Matriz de Pruebas MEA 03.01.

DOMINIO: Supervisar, evaluar y valorar		
MEA 03. Supervisar, evaluar y valorar la conformidad con los requerimientos externos		
Objetivo de Control Detallado	**Revisión a través de:**	**Descripción de la Prueba**
MEA 03.01 Identificar requisitos externos de cumplimiento Identificar y supervisar, de manera continuada, cambios en las legislaciones y regulaciones tanto locales como internacionales, así como otros requisitos externos de obligado cumplimiento en el área de TI. (COBIT 5, 2012) Pag. 214 **Actividades** • Asignar la responsabilidad de identificar y supervisar los cambios legales y regulatorios y otros requisitos contractuales externos aplicables a la utilización de recursos de TI y al procesamiento de la información dentro de las operaciones de negocio y de TI (COBIT 5, 2012) Pag. 214 • Identificar y valorar la totalidad de los posibles requisitos de cumplimiento y su	Evaluación de Controles: Se llevó a cabo una revisión de los requisitos externos e internos sobre el área de TI. Se lleva a cabo una revisión de las legislaciones y regulaciones de la institución sobre el área de TI Probando que: No existe ninguno procedimiento en el que conste las legislaciones y regulación en el área de TI sobre la institución. Se intuye que el área encargada tiene conocimiento de los requisitos externos y lo cumple. No existe documentación	Entrevista al administrador del departamento de sistemas, talento humano y rector de la institución. Entrevista al gerente de TI.

DOMINIO: Supervisar, evaluar y valorar		
MEA 03. Supervisar, evaluar y valorar la conformidad con los requerimientos externos		
Objetivo de Control Detallado	**Revisión a través de:**	**Descripción de la Prueba**
impacto sobre las actividades de TI en ámbitos como los flujos de datos, la privacidad, los controles internos, los informes financieros, la regulación sectorial, la propiedad intelectual y la seguridad en el trabajo. (COBIT 5, 2012) Pag. 214. • Mantener un inventario actualizado de los requisitos legales, regulatorios y contractuales aplicables, su impacto y las acciones necesarias. (COBIT 5, 2012) Pag. 214. • Mantener un registro general consolidado de los requisitos externos de cumplimiento que afecten a la empresa. (COBIT 5, 2012) Pag. 214		

4.2.1.3 Recolección de documentación: manuales de procedimientos, funciones y políticas

No existe dentro de la Institución ninguna documentación referente a las áreas de TI.
Se procederá a realizar las respectivas recomendaciones en el siguiente capítulo.

5.2 Cronograma de Auditoría

ACTIVIDAD / SEMANA	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Descripción de la Organización Administrativa															
Infraestructura actual de la red															
Evaluación de Riesgos de la Gestion de Seguridad de la Red Informática															
Elaboracion del Plan de Auditoria															
Definición del alcance de la Auditoría															
Proceso en el dominio de supervisar, evaluar y valorar															
Puesta en Marcha del Plan de Auditoría															
Elaboracion del Programa de Auditoría															
Elaboración de Matriz de Pruebas															
Recolección de documentación: manuales de procedimientos, funciones y políticas															
Evaluación y Análisis de las pruebas realizadas															
Elaboración del Informe Preliminar															
Discución del Informe Preliminar															
Elaboración del Informe Final															

Observación:

Como observación crítica se puede señalar que no existe documentación referente al área de Tecnologías de Información en la Unidad Educativa “La Asunción”.

Conclusión:

En este capítulo se realizó la Auditoría en el dominio de supervisar, evaluar y valorar, con el objetivo de control de “MEA 03.01 Identificar requisitos externos de cumplimiento”, teniendo como resultados desfavorables la falta de documentación, procedimientos de legislaciones y regulaciones en el área de TI de la Institución Educativa Particular “La Asunción”, esto implica un riesgo muy grande ya que el departamento de sistemas estará obligado a cumplir ninguna ley ni política con respecto a la seguridad de las tecnologías de información, y en el caso de cambio de personal no sabrá qué seguridad se ha utilizado en la tecnologías de información; por lo tanto se procederá a realizar recomendaciones de las legislaciones y regulaciones que se debería tomar en cuenta dentro de la institución.

CAPÍTULO 5

Informes de Auditoría

5.1 Análisis de los resultados obtenido

Una vez efectuada las pruebas he comprobado que la Institución no cuenta con legislaciones y regulaciones que rijan el cumplimiento en las áreas de TI, por lo tanto se procederá a sugerir políticas de seguridad que rigen a nivel internacional y con ello se realizará una revisión sobre la condición actual de la institución, permitiendo así al final obtener el nivel actual de la gestión de seguridad que se maneja en la institución.

En base a esto se presentará la situación actual del objetivo de control que cumplen los requerimientos y sobre los que no cumplen se harán recomendaciones en el informe final.

5.1.1 Evaluación de Resultados

Cuadro 5.1.1.1 Evaluación de Pruebas MEA 03.01

DOMINIO: Supervisar, evaluar y valorar				
MEA 03. Supervisar, evaluar y valorar la conformidad con los requerimientos externos				
MEA 03.01. Identificar requisitos externos de cumplimiento.				
Revisión a través de:	**Descripción de la Prueba**	**Evaluación**	**Documentos de Soporte**	**Recomendación**
Evaluación de Controles: Se lleva a cabo una revisión de los requisitos externos e internos sobre el área de TI. Se lleva a cabo una revisión de las legislaciones y regulaciones de la institución sobre el área de TI Probando que: No existe ninguno procedimiento en el que conste las legislaciones y regulaciones en el área de TI sobre la institución. Se intuye que el área encargada tiene conocimiento	Entrevista al administrador del departamento de sistemas, talento humano y rector de la institución. Entrevista al gerente de TI.	NO EFECTIVO	No existe documento de soporte.	Realizar un documento que contenga un reglamento sobre el cumplimiento legal y regulatorio, tanto local como internacional en el área de las tecnologías de la información dentro de la Institución Educativa

5.2. Análisis de resultados

En base a la evaluación de la gestión de seguridad de la red informática se determinó que existe un bajo porcentaje de cumplimiento de las condiciones necesarias para la seguridad ante riesgos de la red.
Y en base a la evaluación de las pruebas efectuadas en el dominio de supervisar, evaluar y valorar, en el objetivo de control detallado "MEA 03.01 Identificar requisitos externos de cumplimiento" no cuenta con ninguna documentación de legislaciones y regulaciones en el área de TI de la Institución Educativa Particular "La Asunción", tomando en cuenta que esto implica muchos riesgos dentro de la institución.

La carencia de documentación no permite que el departamento de sistemas se rija a leyes y políticas propuestas dentro de la institución. El rector de la Institución supone el buen trabajo de los integrantes del departamento de sistemas, pero no tiene documentación que respalde la seguridad ni el trabajo realizado dentro de la Institución en el área de TI.

5.3 Informe final de la Auditoría

Los informes preliminar y final que se presentan a continuación, tuvieron su discusión y análisis previo con el responsable del área de T.I. dentro de la Institución, es decir con el departamento de sistemas.

5.3.1 Informe preliminar de la Auditoría y su discusión

Alcance de la Auditoría:

El siguiente trabajo de Auditoría aplicará COBIT como metodología para la evaluación y análisis de los diferentes procesos y controles que se aplican en el área de la tecnología de la información.

La Auditoría se centrará en el análisis de la gestión de la seguridad informática que es aplicada actualmente en la red de datos de la Institución Educativa "La Asunción".

Se identificarán las debilidades existentes y sus riesgos potenciales, se expondrán una serie de conclusiones sobre los actuales procedimientos y controles de seguridad así como recomendaciones para el mejoramiento de la gestión de seguridad Informática.

Objetivos de la Auditoría:

Analizar y diagnosticar la actual gestión de seguridad en la red de datos de la Institución Educativa "La Asunción".

Plantear las mejoras para la gestión de la seguridad de la red de datos.

Proponer actividades que ayudarán a identificar los controles que se requieren para garantizar la seguridad de la información.

Temas considerados críticos

Requisitos externos de cumplimiento

Observación: No existe documentación de legislaciones y regulaciones en el área de TI de la Institución Educativa.

Recomendaciones: Elaborar la documentación correspondiente a las legislaciones y regulaciones del área de TI, que rijan en la Unidad Educativa.

Resultado de la discusión con el responsable del área de TI: Dentro del departamento de sistemas no existe documentación ni de procesos, ni de regulaciones; sin embargo existe procedimientos para el uso de laboratorios se hace chequeo antes de clases y después de clases, y a través de bitácora se registra de que hora a que hora se utilizó el aula en caso de que haber algún inconveniente con algún equipo del laboratorio. Esta política se la conoce de manera verbal, pero no existe ninguna documentación que forme parte de las políticas de la institución.

Evaluación de Riesgos

Observación: No existe documentación de políticas de TI, ni de confidencialidad con respecto a los servidores y PC, y equipos de conexión de red.
Con respecto a las aplicaciones en red tanto las de escritorio como la web no guardan confidencialidad de sus cuentas y contraseñas; también estas aplicaciones no tienen todos los campos validados, esto crea inseguridad en la información proporcionada a través de las aplicaciones en red.

Recomendaciones: Elaborar documentación de políticas que rijan el área de TI dentro de la institución, también se recomienda cifrar las claves de los usuarios *(estudiantes, padres de familia y administrativos)*.
Es necesario también validar todos los campos mostrados al usuario para evitar el ingreso de información no confiable.

Resultado de la discusión con el responsable del área de TI:
El responsable del área de TI manifiesta que no existe una documentación de políticas, pero existe una documentación de acta entrega y recepción con respecto a entrega de equipos en caso de existir algún problema en el equipo, pero esto no está planteado en ninguna documentación, la cual sea de conocimiento de los docentes; supo explicar también que nunca le han hecho firmar ninguna política de confidencialidad, simplemente su ética profesional lo hace actuar con responsabilidad en su puesto de trabajo.
Con respecto a la encriptación de claves del contraseñas de los usuarios, nunca lo habían planteado dentro del área, ya que el recibió un programa y una base de datos ya desarrollada; pero aun así el estaría dispuesto a elaborar la encriptación correspondiente en la base de datos.
Con respecto a la validación sostiene que la mayoría de los campos están validados, por lo general los que consideraban “verdaderamente necesarios”, por ejemplo la cédula, el mail, etc; pero por ejemplo el nombre depende exclusivamente de la digitación del usuario.

5.3.2 Informe final de la Auditoría

Anexo #5.docx.

5.4 Ejecución de algunos procesos

A continuación se preponen la realización del proceso “MEA 03.01 Identificar requisitos externos de cumplimiento”, para obtener una mejora en el control de la seguridad, sin embargo es necesario aclarar que este proceso se encuentra fuera de COBIT, nos basaremos en las legislaciones y regulaciones planteadas a nivel internacional, en Latinoamérica, por lo que el procesos que se proponen a continuación es una contribución adicional basados en los resultados obtenidos para mejorar el control existente en la Institución Educativa.

Para este proceso se consideran las siguientes legislaciones y regulaciones.

Anexo #6.docx

Conclusión:

En la elaboración de este capítulo se realizó el análisis de resultados obtenidos en la Auditoría en el dominio de supervisar, evaluar y valorar, con el objetivo de control de "MEA 03.01 Identificar requisitos externos de cumplimiento", teniendo como resultado el informe preliminar que fue expuesto al responsable de TI de la Institución y el informe final que fue entregado al Rector de la Institución.

También se sugirió procedimientos de legislaciones y regulaciones en el área de TI para la Institución Educativa Particular "La Asunción"; basándonos en regulaciones internacionales a nivel de Latinoamérica.

Al informe final se adjuntó también los procedimientos de legislaciones y regulaciones.

CAPÍTULO 6

Conclusiones y Recomendaciones

6.1 Conclusiones

Puedo concluir recalcando los beneficios que nos brinda COBIT en la realización de una Auditoría en todo ámbito empresarial; COBIT proporciona un marco de referencia amplio, que ayuda a las empresas a alcanzar sus metas y ofrece valor, a través de una gobernabilidad y gestión eficaz de las TI de la empresa. (COBIT 5, 2000).

Define un punto de partida de la gobernabilidad y las actividades de gestión con las necesidades de las partes interesadas relacionadas con las TI de la empresa. (COBIT 5, 2000).

Crea una visión más holística, integrada y completa de la gobernabilidad y gestión empresarial de TI, que es consistente, ofrece una visión extremo a extremo en las materias relacionadas a TI.
Crea un lenguaje común entre TI y el negocio.
Es consistente con los estándares de gobernabilidad corporativos (COBIT 5, 2000).

COBIT enfoca sus documentos y guías para la Auditoría en los Procesos COBIT. COBIT 5 a diferencia de COBIT 4 nos da una guía orientada únicamente a los procesos conocida como COBIT Catalizadores, que es la que se utilizó para la realización de esta Auditoría, vale recalcar que estos procesos no siempre están enfocados exactamente con el área informática que se desea auditar, de aquí que sea necesario realizar un trabajo de investigación y de documentación adicional por parte del auditor para lograr la concatenación con los Objetivos COBIT relacionados y el área a auditar. (COBIT 5, 2012).

Una vez resaltada la importancia de COBIT en la Auditoría realizada en la Institución Educativa Particular “La Asunción” podemos partir diciendo que de la discusión del informe preliminar de la Auditoría se concluye que no existe una conciencia más formal por parte de la Gerencia de T.I. para asegurar la correcta gestión de la seguridad.
El no tener determinados correctamente los recursos críticos de T.I. puede acarrear el no contar con planes de continuidad adecuados y por lo tanto propensos a sufrir un ataque de seguridad, pérdida de información, etc. De los cuales será casi imposible recuperarse sin causar pérdidas económicas a la organización.

En La Unidad Educativa Particular “La Asunción”, debido a que su objetivo primordial es la de la Educación; esto ha permitido que ciertas áreas de seguridad informática sean descuidadas y aun cuando no se han convertido en un problema crítico, están a tiempo de cubrir las recomendaciones y estándares de seguridad sugeridos en esta Auditoría, a pesar de que no se ha podido cubrir todos los procesos que COBIT nos recomienda.

6.2. Recomendaciones

Fuera de gran ayuda realizad una Auditoría que cubra los demás procesos faltantes dentro de la Institución educativa para cubrir debilidades existentes dentro de la misma.

Elaborar la documentación correspondiente a las legislaciones y regulaciones del área de TI, que rijan en la Unidad Educativa; toda área de TI tiene que asegurar al usuario la confidencialidad, la integridad y/o la disponibilidad de las tecnologías de información.
Los riesgos son los mismos con respecto a la carencia de documentación, esto no crea seguridad en el área de las tecnologías de Información.

Esto incluye definir procedimientos específicos para el establecimiento de controles efectivos dentro de la gestión de seguridad, como la implementación de revisiones de posibles violaciones a la seguridad y accesos no autorizados.

Con respecto a las claves guardadas en la base de datos es importante cifrarlas con la finalidad de asegurar integridad de la información ya que pueden sufrir de hurto, adulteración, fraude, modificación, revelación, pérdida, sabotaje, vandalismo, crackers, hackers, falsificación, robo de contraseñas, alteraciones etc; es importante también crear procedimientos de seguridad que se base en los estándares de seguridad y políticas de contraseñas.

Con respecto a los campos no validados, es importante recordar que todos los campos son importantes no solo los de cedula y mail, el objetivo es garantizar que la información proporcionada es confiable; en el caso del campo “nombre” se puede ingresar números o caracteres especiales esto rompería con el objetivo de contener información confiable; no se puede confiar ciegamente en el usuario ya que puede haber errores por descuido, falta de seriedad, o un ordenador intentando acceder a la información de la Institución.

Finalmente, se recomienda a COBIT como una herramienta para realizar el análisis y evaluación de los puntos críticos de la organización para futuras Auditorías, tomando como base la guía de procesos catalizadores.

Si bien COBIT brinda en sus documentos las herramientas necesarias para el proceso de Auditoría, es conveniente tener un conocimiento básico de cómo desarrollar una Auditoría informática y de esta manera explotar mejor todas las bondades de COBIT.

Anexo #1

EQUIPOS DE COMPUTACIÓN

Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
1	UEAIGEC1306000008	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
2	UEAIGEC1306000011	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
3	UEAIGEC1306000014	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
4	UEAIGEC1306000019	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
5	UEAIGEC1306000024	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
6	UEAIGEC1306000006	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
7	UEAIGEC1306000007	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
8	UEAIGEC1306000010	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
9	UEAIGEC1306000018	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
10	UEAIGEC1306000020	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
11	UEAIGEC1306000027	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
12	UEAIGEC1306000028	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
13	UEAIGEC1306000016	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
14	UEAIGEC1306000017	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
15	UEAIGEC1306000022	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
16	UEAIGEC1306000023	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
17	UEAIGEC1306000005	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
18	UEAIGEC1306000009	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
19	UEAIGEC1306000012	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
20	UEAIGEC1306000013	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
21	UEAIGEC1306000015	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
22	UEAIGEC1306000021	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
23	UEAIGEC1306000025	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
24	UEAIGEC1308000001	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
25	UEAIGEC1308000002	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
26	UEAIGEC1308000003	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
27	UEAIGEC1308000004	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
28	UEAIGEC1308000005	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
29	UEAIGEC1308000006	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
30	UEAIGEC1308000007	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
31	UEAIGEC1308000008	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
32	UEAIGEC1308000009	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
33	UEAIGEC1308000010	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
34	UEAIGEC1308000010	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
35	UEAIGEC1308000011	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
36	UEAIGEC1308000012	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
37	UEAIGEC001327	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
38	UEAIGEC001335	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
39	UEA0017000003	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
40	UEAIGEC001120	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER

Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
41	UEAIGEC001150	CPU CLON ATX	327,55	SERRANO TAPIA MARCELA
42	UEAIGEC001161	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
43	UEAIGEC001142	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
44	UEAIGEC001167	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
45	UEAIGEC1312000057	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
46	UEAIGEC1312000057	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
47	UEAIGEC1312000058	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
48	UEAIGEC1312000058	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
49	UEAIGEC1312000058	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
50	UEAIGEC1312000059	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
51	UEAIGEC1312000059	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
52	UEAIGEC1312000059	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
53	UEAIGEC1312000060	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
54	UEAIGEC1312000060	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
55	UEAIGEC1312000060	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
56	UEAIGEC1312000061	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
57	UEAIGEC1312000061	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
58	UEAIGEC1312000061	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
59	UEAIGEC1312000062	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
60	UEAIGEC1312000062	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
61	UEAIGEC1312000062	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
62	UEAIGEC1312000063	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
63	UEAIGEC1312000063	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
64	UEAIGEC1312000063	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
65	UEAIGEC1312000064	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
66	UEAIGEC1312000064	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
67	UEAIGEC1312000064	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
68	UEAIGEC1312000065	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
69	UEAIGEC1312000065	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
70	UEAIGEC1312000065	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
71	UEAIGEC1312000066	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
72	UEAIGEC1312000066	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
73	UEAIGEC1312000066	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
74	UEAIGEC1312000067	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
75	UEAIGEC1312000067	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
76	UEAIGEC1312000067	CPU HP DX2400	409,00	SARMIENTO POLO PABLO
77	UEAIGEC0917000001	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
78	UEAIGEC0917000002	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
79	UEAIGEC001029	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
80	UEAIGEC001045	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
81	UEAIGEC001252	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
82	UEAIGEC000985	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
83	UEAIGEC001261	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
84	UEAIGEC001127	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER

Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
85	UEAIGEC001114	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
86	UEAIGEC001106	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
87	UEAIGEC001242	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
88	UEA0004000001	CPU CLON ATX	390,00	MONTERO ORTIZ KLEVER
89	UEAIGEC001367	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
90	UEAIGEC001284	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
91	UEAIGEC001394	CPU CLON ATX	390,00	MONTERO ORTIZ KLEVER
92	UEAIGEC1049000002	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
93	UEAIGEC1049000003	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
94	UEAIGEC1049000001	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
95	UEAIGEC1174000001	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
96	UEAIGEC1174000003	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
97	UEAIGEC1174000006	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
98	UEAIGEC1174000007	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
99	UEAIGEC1174000008	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
100	UEAIGEC1174000011	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
101	UEAIGEC1174000012	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
102	UEAIGEC1174000016	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
103	UEAIGEC1174000018	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
104	UEAIGEC1174000021	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
105	UEAIGEC1174000022	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
106	UEAIGEC1174000002	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
107	UEAIGEC1174000004	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
108	UEAIGEC1174000009	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
109	UEAIGEC1174000010	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
110	UEAIGEC1174000014	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
111	UEAIGEC1174000015	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
112	UEAIGEC1174000019	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
113	UEAIGEC1174000020	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
114	UEAIGEC1174000005	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
115	UEAIGEC1174000013	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
116	UEAIGEC1174000017	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
117	UEAIGEC1174000023	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
118	UEAIGEC1134000001	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
119	UEAIGEC1134000002	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
120	UEAIGEC1134000001	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
121	UEAIGEC1134000002	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER

Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
122	UEAIGEC000915	LP TOSHIBA L35	627,55	MONTERO ORTIZ KLEVER
123	UEAIGEC001400	LP SAMSUNG	627,55	MONTERO ORTIZ KLEVER
124	UEAIGEC001401	LP SAMSUNG	627,55	MONTERO ORTIZ KLEVER
125	UEAIGEC001398	LP SAMSUNG	627,55	MONTERO ORTIZ KLEVER
126	UEAIGEC001399	LP SAMSUNG	627,55	MONTERO ORTIZ KLEVER
127	UEAIGEC001226	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
128	UEAIGEC001178	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
129	UEAIGEC001018	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
130	UEAIGEC000922	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
131	UEAIGEC001052	CPU NEXXUS ATX	327,55	AQUILLA TERAN WALTER
132	UEAIGEC001231	CPU NEXXUS ATX	327,55	SANCHEZ TAMARIZ TANIA
133	UEAIGEC000903	CPU NEXXUS ATX	327,55	MONTERO ORTIZ KLEVER
134	UEAIGEC0990000007	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
135	UEAIGEC0990000008	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
136	UEAIGEC0990000013	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
137	UEAIGEC0990000014	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
138	UEAIGEC0990000015	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
139	UEAIGEC0990000001	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
140	UEAIGEC0990000004	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
141	UEAIGEC0990000005	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
142	UEAIGEC0990000012	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
143	UEAIGEC0990000016	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
144	UEAIGEC0990000019	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
145	UEAIGEC0990000021	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
146	UEAIGEC0990000023	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
147	UEAIGEC0990000024	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
148	UEAIGEC0990000003	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
149	UEAIGEC0990000006	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
150	UEAIGEC0990000009	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
151	UEAIGEC0990000010	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
152	UEAIGEC0990000022	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
153	UEAIGEC0990000002	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
154	UEAIGEC0990000011	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
155	UEAIGEC0990000017	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
156	UEAIGEC0990000018	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
157	UEAIGEC0990000020	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
158	UEA0028000017	CPU CLON ATX	390,00	TAPIA CARDENAS EDGAR
159	UEA0028000018	CPU CLON ATX	390,00	TAPIA CARDENAS EDGAR
160	UEA0028000021	CPU CLON ATX	390,00	TAPIA CARDENAS EDGAR
161	UEA0028000014	CPU CLON ATX	390,00	TAPIA CARDENAS EDGAR
162	UEA0028000016	CPU CLON ATX	390,00	TAPIA CARDENAS EDGAR
163	UEA0028000020	CPU CLON ATX	390,00	TAPIA CARDENAS EDGAR

Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
164	UEA0028000019	CPU CLON ATX	390,00	TAPIA CARDENAS EDGAR
165	UEA0028000022	CPU CLON ATX	390,00	TAPIA CARDENAS EDGAR
166	UEA0028000023	CPU CLON ATX	390,00	TAPIA CARDENAS EDGAR
167	UEA0029000004	CPU CLON ATX	390,00	TAPIA CARDENAS EDGAR
168	UEA0028000015	CPU CLON ATX	390,00	TAPIA CARDENAS EDGAR
169	UEA0029000001	CPU CLON ATX	390,00	TAPIA CARDENAS EDGAR
170	UEAIGEC001375	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
171	UEA0030000003	CPU CLON ATX	390,00	TAPIA CARDENAS EDGAR
172	UEAIGEC001312	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
173	UEAIGEC001289	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
174	UEAIGEC001030	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
175	UEAIGEC001073	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
176	UEAIGEC000995	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
177	UEAIGEC001378	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
178	UEAIGEC001096	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
179	UEAIGEC001255	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
180	UEAIGEC001004	CPU CLON ATX	327,55	SARMIENTO POLO PABLO
181	UEAIGEC001268	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
182	UEAIGEC001407	LP HP GA-2200LA	627,55	BARRERA TELLO MARIELA
183	UEAIGEC001406	LP HP HP455	627,55	BARRERA TELLO MARIELA
184	UEAIGEC1308000059	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
185	UEAIGEC1308000057	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
186	UEAIGEC1308000058	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
187	UEAIGEC1308000058	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
188	UEAIGEC1308000056	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
189	UEAIGEC1308000049	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
190	UEAIGEC1308000054	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
191	UEAIGEC1308000060	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
192	UEAIGEC1308000055	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
193	UEAIGEC1308000052	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
194	UEAIGEC1308000051	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
195	UEAIGEC1308000050	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
196	UEAIGEC1308000053	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
197	UEAIGEC001324	CPU CLON ATX	327,55	MONTERO ORTIZ KLEVER
198	UEAIGEC001332	CPU CLON ATX	327,55	TAPIA CARDENAS EDGAR
199	UEAIGEC001444	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
200	UEAIGEC001445	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
201	UEAIGEC001446	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
202	UEAIGEC001449	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
203	UEAIGEC001450	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
204	UEAIGEC001451	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
205	UEAIGEC001452	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
206	UEAIGEC001453	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
207	UEAIGEC001454	CPU CLON ATX	377,00	BARRERA TELLO MARIELA

Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
208	UEAIGEC001455	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
209	UEAIGEC001456	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
210	UEAIGEC001457	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
211	UEAIGEC001458	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
212	UEAIGEC001459	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
213	UEAIGEC001460	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
214	UEAIGEC001461	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
215	UEAIGEC001462	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
216	UEAIGEC001463	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
217	UEAIGEC001464	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
218	UEAIGEC001465	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
219	UEAIGEC001466	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
220	UEAIGEC001467	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
221	UEAIGEC001468	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
222	UEAIGEC001469	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
223	UEAIGEC001470	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
224	UEAIGEC001471	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
225	UEAIGEC001472	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
226	UEAIGEC001473	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
227	UEAIGEC001474	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
228	UEAIGEC001475	CPU CLON ATX	377,00	BARRERA TELLO MARIELA
229	UEAIGEC001498	CPU CLON ATX	377,00	RODRIGO CABRERA
230	UEAIGEC001499	CPU CLON ATX	377,00	RODRIGO CABRERA
231	UEAIGEC001500	CPU CLON ATX	377,00	RODRIGO CABRERA
232	UEAIGEC001501	CPU CLON ATX	377,00	RODRIGO CABRERA
233	UEAIGEC001502	CPU CLON ATX	377,00	RODRIGO CABRERA
234	UEAIGEC001503	CPU CLON ATX	377,00	RODRIGO CABRERA
235	UEAIGEC001504	CPU CLON ATX	377,00	RODRIGO CABRERA
236	UEAIGEC001505	CPU CLON ATX	377,00	RODRIGO CABRERA
237	UEAIGEC001506	CPU CLON ATX	377,00	RODRIGO CABRERA
238	UEAIGEC001507	CPU CLON ATX	377,00	RODRIGO CABRERA
239	UEAIGEC001508	CPU CLON ATX	377,00	RODRIGO CABRERA
240	UEAIGEC001509	CPU CLON ATX	377,00	RODRIGO CABRERA
241	UEAIGEC001510	CPU CLON ATX	377,00	RODRIGO CABRERA
242	UEAIGEC001511	CPU CLON ATX	377,00	RODRIGO CABRERA
243	UEAIGEC001512	CPU CLON ATX	377,00	RODRIGO CABRERA
244	UEAIGEC001513	CPU CLON ATX	377,00	RODRIGO CABRERA
245	UEAIGEC001514	CPU CLON ATX	377,00	RODRIGO CABRERA
246	UEAIGEC001515	CPU CLON ATX	377,00	RODRIGO CABRERA
247	UEAIGEC001516	CPU CLON ATX	377,00	CARRASCO LUCIA
248	UEAIGEC001517	CPU CLON ATX	377,00	CARRASCO LUCIA
249	UEAIGEC001518	CPU CLON ATX	377,00	CARRASCO LUCIA
250	UEAIGEC001519	CPU CLON ATX	377,00	CARRASCO LUCIA
251	UEAIGEC001520	CPU CLON ATX	377,00	CARRASCO LUCIA

Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
252	UEAIGEC001521	CPU CLON ATX	377,00	CARRASCO LUCIA
253	UEAIGEC001522	CPU CLON ATX	377,00	CARRASCO LUCIA

NETWORKING

Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
1	UEAIGEC1311000003	CISCO 1760/W	$ 350,00	MONTERO ORTIZ KLEVER
2	UEAIGEC1082000002	PATH PANEL 48P	$ 100,00	SARMIETO POLO PABLO
3	UEAIGEC1082000001	PATH PANEL 48P	$ 100,00	SARMIETO POLO PABLO
4	UEA0011000007	CISCO 2810/W	$1.050,00	VANEGAS DELGADO VANESSA
5	UEAIGEC001085	UPS-TL 3Kva	$1.000,00	SARMIETO POLO PABLO
6	UEAIGEC001414	RB1100AHX2	$690,00	MARIELA BARRERA
7	UEAIGEC0973000002	SWITCH 3COM / HP P2024	$ 100,00	SARMIETO POLO PABLO
8	UEAIGEC0973000003	SWITCH 3COM / HP P2024	$ 100,00	SARMIETO POLO PABLO
9	UEAIGEC0973000001	SWITCH 3COM / HP P2024	$ 100,00	SARMIETO POLO PABLO
10	UEA0019000007	SWITCH 3COM / HP V1905-24 PORT	$ 185,00	VANEGAS DELGADO VANESSA
11	UEA0017000005	SWITCH 3COM / HP V1905-24 PORT	$ 185,00	VANEGAS DELGADO VANESSA
12	UEA0011000006	SWITCH 3COM / HP B2226-24 PORT	$ 185,00	VANEGAS DELGADO VANESSA
13	UEAIGEC001086	KVM 8P D-LINK SWITCH	$ 250,00	SARMIETO POLO PABLO
14	UEAIGEC001433	SWITCH 3COM / HP 2250SPF	$ 250,00	JOSE GALARZA
15	UEAIGEC001434	SWITCH 3COM / HP 2250SPF	$ 250,00	JOSE GALARZA
16	UEAIGEC001435	SWITCH 3COM / HP 2226SFP	$ 250,00	JOSE GALARZA
17	UEAIGEC001436	SWITCH 3COM / HP 2226SFP	$ 250,00	JOSE GALARZA
18	UEAIGEC001437	SWITCH 3COM / HP 2226SFP	$ 250,00	JOSE GALARZA
19	UEAIGEC001438	SWITCH 3COM / HP 2226SFP	$ 250,00	JOSE GALARZA
20	UEAIGEC001439	SWITCH 3COM / HP 2226SFP	$ 250,00	JOSE GALARZA
21	UEAIGEC001440	SWITCH 3COM / HP 2226SFP	$ 250,00	JOSE GALARZA
22	UEAIGEC001441	SWITCH 3COM / HP 2226SFP	$ 250,00	JOSE GALARZA
23	UEAIGEC001442	SWITCH 3COM / HP 2226SFP	$ 250,00	JOSE GALARZA
24	UEAIGEC001476	SWITCH 3COM / HP 2916SPF	$ 250,00	JOSE GALARZA
25	UEAIGEC001530	SWITCH 3COM / HP 2226SFP	$ 250,00	JOSE GALARZA

SERVERS

Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
1	UEAIGEC1087000001	SERVER QCORE CLON 1P	$ 390,55	SARMIENTO POLO PABLO
2	UEAIGEC1087000002	SERVER QCORE CLON 1P	$ 390,55	SARMIENTO POLO PABLO
3	UEAIGEC001420	SERVIDOR HP DL360Ge 1P	$ 2.800,00	BARRERA TELLO MARIELA
4	UEAIGEC1312000069	SERVIDOR HP ML 160 G6 RACK 2 P	$1.607,00	SARMIENTO POLO PABLO
5	UEAIGEC001083	SERVIDOR HP ML 150 G2 1P	$1.669,92	SARMIENTO POLO PABLO
6	UEAIGEC001084	SERVDIDOR IBM 206 1P	$2.093,28	SARMIENTO POLO PABLO

MONITORES

Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
1	UEAIGEC000950	MONITOR 15" LG / CRT	$ 112,05	SARMIENTO POLO PABLO
2	UEAIGEC000949	MONITOR 15" LG / CRT	$ 112,05	SARMIENTO POLO PABLO
3	UEAIGEC001128	MONITOR 15" SAMSUNG / CRT	$ 99,00	LOPEZ JARA JORGE EUGENIO
4	UEAIGEC001115	MONITOR 15" SAMSUNG / CRT	$ 99,00	MONTERO ORTIZ KLEVER
5	UEAIGEC001262	MONITOR 15" SAMSUNG / CRT	$ 99,00	PULLA GUERRERO MARIA PIEDAD
6	UEAIGEC001107	MONITOR 15" SAMSUNG / CRT	$ 99,00	MONTERO ORTIZ KLEVER
7	UEAIGEC000948	MONITOR 15" SAMSUNG / CRT	$ 99,00	SARMIENTO POLO PABLO
8	UEAIGEC001339	MONITOR 17" LG / LCD	$ 201,60	TOBAR CORONEL ROSARIO
9	UEAIGEC001320	MONITOR 17" LG / LCD	$ 201,60	MONTERO ORTIZ KLEVER
10	UEAIGEC001361	MONITOR 17" AOC / CRT	$ 156,82	MONTERO ORTIZ KLEVER
11	UEAIGEC000946	MONITOR 15" LG / CRT	$ 145,00	SARMIENTO POLO PABLO
12	UEAIGEC001099	MONITOR 15" / CRT	$ 137,25	MONTERO ORTIZ KLEVER
13	UEAIGEC001121	MONITOR 15" / CRT	$ 137,25	MONTERO ORTIZ KLEVER
14	UEAIGEC001239	MONITOR 15" / CRT	$ 137,25	MONTERO ORTIZ KLEVER
15	UEAIGEC1307000003	MONITOR 15" / CRT	$ 137,25	MONTERO ORTIZ KLEVER
16	UEAIGEC000947	MONITOR 15" SAMSUNG / CRT	$ 150,75	SARMIENTO POLO PABLO
17	UEAIGEC001005	MONITOR 17" SAMSUNG / LCD	$ 236,25	MONTERO ORTIZ KLEVER
18	UEAIGEC000906	MONITOR 17" SAMSUNG / LCD	$ 236,25	MONTERO ORTIZ KLEVER
19	UEAIGEC000923	MONITOR 17" SAMSUNG / LCD	$ 236,25	MONTERO ORTIZ KLEVER
20	UEAIGEC001227	MONITOR 17" SAMSUNG / LCD	$ 236,25	MONTERO ORTIZ KLEVER
21	UEAIGEC001234	MONITOR 17" SAMSUNG / LCD	$ 236,25	MONTERO ORTIZ KLEVER
22	UEAIGEC001019	MONITOR 17" SAMSUNG / LCD	$ 236,25	MONTERO ORTIZ KLEVER
23	UEAIGEC001053	MONITOR 17" SAMSUNG / LCD	$ 236,25	MONTERO ORTIZ KLEVER
24	UEAIGEC001179	MONITOR 17" SAMSUNG / LCD	$ 236,25	MONTERO ORTIZ KLEVER
25	UEAIGEC1312000004	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
26	UEAIGEC1312000005	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
27	UEAIGEC1312000015	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
28	UEAIGEC1312000016	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
29	UEAIGEC1312000021	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
30	UEAIGEC1312000022	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
31	UEAIGEC1312000023	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
32	UEAIGEC1312000024	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
33	UEAIGEC1312000028	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
34	UEAIGEC1312000032	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
35	UEAIGEC1312000033	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
36	UEAIGEC1312000034	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
37	UEAIGEC1312000001	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
38	UEAIGEC1312000002	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
39	UEAIGEC1312000003	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO

Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
40	UEAIGEC1312000007	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
41	UEAIGEC1312000008	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
42	UEAIGEC1312000012	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
43	UEAIGEC1312000013	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
44	UEAIGEC1312000014	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
45	UEAIGEC1312000018	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
46	UEAIGEC1312000020	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
47	UEAIGEC1312000027	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
48	UEAIGEC1312000030	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
49	UEAIGEC1312000031	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
50	UEAIGEC1312000010	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
51	UEAIGEC1312000011	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
52	UEAIGEC1312000017	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
53	UEAIGEC1312000026	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
54	UEAIGEC1312000029	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
55	UEAIGEC1312000006	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
56	UEAIGEC1312000009	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
57	UEAIGEC1312000019	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
58	UEAIGEC1312000025	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
59	UEAIGEC1312000035	MONITOR 17" HP / LCD	$ 149,00	SARMIENTO POLO PABLO
60	UEAIGEC001287	MONITOR 19" LG / LCD	$ 198,00	MONTERO ORTIZ KLEVER
61	UEAIGEC0991000001	MONITOR 19" LG / LCD	$ 198,00	SARMIENTO POLO PABLO
62	UEAIGEC0991000002	MONITOR 19" LG / LCD	$ 198,00	SARMIENTO POLO PABLO
63	UEAIGEC001143	MONITOR 19" LG / LCD	$ 198,00	MONTERO ORTIZ KLEVER
64	UEAIGEC001309	MONITOR 19" LG / LCD	$ 198,00	CALLE COBOS CLARA MARIA
65	UEAIGEC001151	MONITOR 19" LG / LCD	$ 198,00	ARGUDO VICUNA PATRICIA
66	UEAIGEC001371	MONITOR 17" LG / LCD	$ 181,00	SALINAS SANTACRUZ MERCEDES
67	UEA0028000011	MONITOR 18.5" LG / LCD	$ 105,00	TAPIA CARDENAS EDGAR GONZALO
68	UEA0028000008	MONITOR 18.5" LG / LCD	$ 105,00	TAPIA CARDENAS EDGAR GONZALO
69	UEA0028000009	MONITOR 18.5" LG / LCD	$ 105,00	TAPIA CARDENAS EDGAR GONZALO
70	UEA0028000007	MONITOR 18.5" LG / LCD	$ 105,00	TAPIA CARDENAS EDGAR GONZALO
71	UEA0028000006	MONITOR 18.5" LG / LCD	$ 105,00	TAPIA CARDENAS EDGAR GONZALO
72	UEA0028000010	MONITOR 18.5" LG / LCD	$ 105,00	TAPIA CARDENAS EDGAR GONZALO
73	UEA0028000012	MONITOR 18.5" LG / LCD	$ 105,00	TAPIA CARDENAS EDGAR GONZALO
74	UEA0029000003	MONITOR 18.5" LG / LCD	$ 105,00	TAPIA CARDENAS EDGAR GONZALO
75	UEA0029000002	MONITOR 18.5" LG / LCD	$ 105,00	TAPIA CARDENAS EDGAR GONZALO
76	UEA0028000004	MONITOR 18.5" LG / LCD	$ 105,00	TAPIA CARDENAS EDGAR GONZALO
77	UEA0028000005	MONITOR 18.5" LG / LCD	$ 105,00	TAPIA CARDENAS EDGAR GONZALO
78	UEAIGEC001395	MONITOR 18.5" LG / LCD	$ 105,00	BARRERA TELLO MARIELA ANTONIETA
79	UEAIGEC001041	MONITOR 14" LG / CRT	$ 150,75	MONTERO ORTIZ KLEVER
80	UEAIGEC001093	MONITOR 14" LG / CRT	$ 150,75	MONTERO ORTIZ KLEVER

Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
81	UEAIGEC001217	MONITOR 14" LG / CRT	$ 150,75	MONTERO ORTIZ KLEVER
82	UEAIGEC001222	MONITOR 14" LG / CRT	$ 150,75	MONTERO ORTIZ KLEVER
83	UEAIGEC001212	MONITOR 14" LG / CRT	$ 150,75	MONTERO ORTIZ KLEVER
84	UEAIGEC0978000001	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
85	UEAIGEC0978000003	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
86	UEAIGEC0978000002	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
87	UEAIGEC001318	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO SAQUICELLA ESTRELLA
88	UEAIGEC1137000001	MONITOR 17" SAMSUNG / LCD	$ 196,00	LOPEZ JARA JORGE EUGENIO
89	UEAIGEC1137000002	MONITOR 17" SAMSUNG / LCD	$ 196,00	LOPEZ JARA JORGE EUGENIO
90	UEAIGEC1177000005	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
91	UEAIGEC1177000009	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
92	UEAIGEC1177000010	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
93	UEAIGEC1177000017	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
94	UEAIGEC1177000018	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
95	UEAIGEC1177000002	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
96	UEAIGEC1177000003	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
97	UEAIGEC1177000004	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
98	UEAIGEC1177000006	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
99	UEAIGEC1177000011	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
100	UEAIGEC1177000020	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
101	UEAIGEC1177000001	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
102	UEAIGEC1177000013	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
103	UEAIGEC1177000014	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
104	UEAIGEC1177000016	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
105	UEAIGEC1177000022	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
106	UEAIGEC1177000023	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
107	UEAIGEC1177000007	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
108	UEAIGEC1177000008	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
109	UEAIGEC1177000012	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
110	UEAIGEC1177000015	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
111	UEAIGEC1177000019	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
112	UEAIGEC1177000021	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
113	UEAIGEC1308000081	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
114	UEAIGEC1308000074	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
115	UEAIGEC1308000075	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
116	UEAIGEC1308000078	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER

Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
117	UEAIGEC1308000082	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
118	UEAIGEC1308000083	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
119	UEAIGEC1308000076	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
120	UEAIGEC1308000073	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
121	UEAIGEC1308000084	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
122	UEAIGEC1308000077	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
123	UEAIGEC1308000079	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
124	UEAIGEC1308000080	MONITOR 17" SAMSUNG / LCD	$ 196,00	MONTERO ORTIZ KLEVER
125	UEAIGEC001418000001	MONITOR 17" SAMSUNG / LCD	$ 196,00	BARRERA TELLO MARIELA ANTONIETA
126	UEAIGEC0992000003	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
127	UEAIGEC0992000007	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
128	UEAIGEC0992000008	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
129	UEAIGEC0992000009	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
130	UEAIGEC0992000015	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
131	UEAIGEC0992000004	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
132	UEAIGEC0992000005	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
133	UEAIGEC0992000013	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
134	UEAIGEC0992000014	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
135	UEAIGEC0992000011	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
136	UEAIGEC0992000012	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
137	UEAIGEC0992000016	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
138	UEAIGEC0992000001	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
139	UEAIGEC0992000002	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
140	UEAIGEC0992000006	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
141	UEAIGEC0992000010	MONITOR 17" SAMSUNG / LCD	$ 196,00	SARMIENTO POLO PABLO
142	UEAIGEC001162	MONITOR 19" SAMSUNG / LCD	$ 198,00	MONTERO ORTIZ KLEVER
143	UEAIGEC001168	MONITOR 19" SAMSUNG / LCD	$ 198,00	MONTERO ORTIZ KLEVER
144	UEAIGEC001074	MONITOR 15" SAMSUNG / CRT	$ 107,00	SARMIENTO POLO PABLO
145	UEAIGEC001310	MONITOR 15" VS / CRT	$ 155,25	SARMIENTO SAQUICELLA ESTRELLA
146	UEAIGEC0975000002	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
147	UEAIGEC0975000012	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
148	UEAIGEC0975000004	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
149	UEAIGEC0975000005	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
150	UEAIGEC0975000006	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
151	UEAIGEC0975000008	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
152	UEAIGEC0975000010	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO

Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
153	UEAIGEC0975000001	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
154	UEAIGEC0975000003	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
155	UEAIGEC0975000007	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
156	UEAIGEC0975000009	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
157	UEAIGEC0975000011	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
158	UEAIGEC0975000013	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
159	UEAIGEC000996	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
160	UEAIGEC000997	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
161	UEAIGEC001034	MONITOR 17" SAMSUNG / LCD	$ 233,80	MONTERO ORTIZ KLEVER
162	UEAIGEC001000	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
163	UEAIGEC000993	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
164	UEAIGEC000998	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
165	UEAIGEC000999	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
166	UEAIGEC000994	MONITOR 17" SAMSUNG / LCD	$ 233,80	SARMIENTO POLO PABLO
167	UEAIGEC001197	MONITOR 14" AOC / CRT	$ 87,00	MONTERO ORTIZ KLEVER
168	UEAIGEC0942000003	MONITOR 15" / CRT	$ 100,00	SARMIENTO POLO PABLO
169	UEAIGEC0942000004	MONITOR 15" / CRT	$ 100,00	SARMIENTO POLO PABLO
170	UEAIGEC0942000001	MONITOR 15" / CRT	$ 100,00	SARMIENTO POLO PABLO
171	UEAIGEC0942000002	MONITOR 15" / CRT	$ 100,00	SARMIENTO POLO PABLO
172	UEAIGEC001388	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
173	UEAIGEC000983	MONITOR 15" SAMSUNG / CRT	$ 103,04	SARMIENTO POLO PABLO
174	UEAIGEC001249	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
175	UEAIGEC000982	MONITOR 15" SAMSUNG / CRT	$ 103,04	SARMIENTO POLO PABLO
176	UEAIGEC000984	MONITOR 15" SAMSUNG / CRT	$ 103,04	SARMIENTO POLO PABLO
177	UEAIGEC1306000175	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
178	UEAIGEC1306000176	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
179	UEAIGEC1306000177	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
180	UEAIGEC1306000178	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
181	UEAIGEC1306000181	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
182	UEAIGEC1306000186	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
183	UEAIGEC1306000187	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
184	UEAIGEC1306000188	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
185	UEAIGEC1306000190	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
186	UEAIGEC1306000193	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
187	UEAIGEC1306000194	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
188	UEAIGEC1306000173	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
189	UEAIGEC1306000174	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO

Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
190	UEAIGEC1306000180	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
191	UEAIGEC1306000183	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
192	UEAIGEC1306000184	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
193	UEAIGEC1306000191	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
194	UEAIGEC1306000195	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
195	UEAIGEC1306000196	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
196	UEAIGEC1306000192	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
197	UEAIGEC1306000179	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
198	UEAIGEC1306000182	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
199	UEAIGEC1306000189	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
200	UEAIGEC1306000174	MONITOR 17" SAMSUNG / LCD	$ 117,53	GALARZA MURILLO JOSE MAURICIO
201	UEAIGEC0981000001	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
202	UEAIGEC0981000002	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
203	UEAIGEC0981000003	MONITOR 17" SAMSUNG / LCD	$ 117,53	SARMIENTO POLO PABLO
204	UEAIGEC0916000002	MONITOR 17" SAMSUNG / LCD	$ 117,53	MONTERO ORTIZ KLEVER
205	UEAIGEC0916000001	MONITOR 17" SAMSUNG / LCD	$ 117,53	MONTERO ORTIZ KLEVER
206	UEAIGEC1210000004	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
207	UEAIGEC1210000013	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
208	UEAIGEC1210000014	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
209	UEAIGEC1210000018	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
210	UEAIGEC1210000019	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
211	UEAIGEC1210000002	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
212	UEAIGEC1210000003	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
213	UEAIGEC1210000008	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
214	UEAIGEC1210000009	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
215	UEAIGEC1210000012	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
216	UEAIGEC1210000005	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
217	UEAIGEC1210000010	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
218	UEAIGEC1210000015	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
219	UEAIGEC1210000017	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
220	UEAIGEC1210000001	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
221	UEAIGEC1210000006	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
222	UEAIGEC1210000007	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
223	UEAIGEC1210000011	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
224	UEAIGEC1210000016	MONITOR 15" SAMSUNG / CRT	$ 103,04	MONTERO ORTIZ KLEVER
225	UEAIGEC001276	MONITOR 15" SAMSUNG / CRT	$ 103,04	ORTEGA GUTIERREZ EDDY BOLIVAR

Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
226	UEA0028000013	MONITOR 18.5" LG / LCD	$ 105,00	TAPIA CARDENAS EDGAR GONZALO
227	UEA0024000015	MONITOR 18.5" LG / LCD	$ 105,00	VANEGAS DELGADO DIANA VANESSA
228	UEA0024000012	MONITOR 18.5" LG / LCD	$ 105,00	VANEGAS DELGADO DIANA VANESSA
229	UEA0024000013	MONITOR 18.5" LG / LCD	$ 105,00	VANEGAS DELGADO DIANA VANESSA
230	UEA0024000014	MONITOR 18.5" LG / LCD	$ 105,00	VANEGAS DELGADO DIANA VANESSA
231	UEAIGEC001523	MONITOR LG 18.5" LCD LED	$ 107,00	CARRASCO LUCIA
232	UEAIGEC001524	MONITOR LG 18.5" LCD LED	$ 107,00	CARRASCO LUCIA
233	UEAIGEC001525	MONITOR LG 18.5" LCD LED	$ 107,00	CARRASCO LUCIA
234	UEAIGEC001526	MONITOR LG 18.5" LCD LED	$ 107,00	CARRASCO LUCIA
235	UEAIGEC001527	MONITOR LG 18.5" LCD LED	$ 107,00	CARRASCO LUCIA
236	UEAIGEC001528	MONITOR LG 18.5" LCD LED	$ 107,00	CARRASCO LUCIA
237	UEAIGEC001529	MONITOR LG 18.5" LCD LED	$ 107,00	CARRASCO LUCIA
238	UEAIGEC001477	MONITOR LG 18.5" LCD LED	$ 107,00	CORNEJO CRISTIAN
239	UEAIGEC001478	MONITOR LG 18.5" LCD LED	$ 107,00	CORNEJO CRISTIAN
240	UEAIGEC001479	MONITOR LG 18.5" LCD LED	$ 107,00	CORNEJO CRISTIAN
241	UEAIGEC001480	MONITOR LG 18.5" LCD LED	$ 107,00	CORNEJO CRISTIAN
242	UEAIGEC001481	MONITOR LG 18.5" LCD LED	$ 107,00	CORNEJO CRISTIAN
243	UEAIGEC001482	MONITOR LG 18.5" LCD LED	$ 107,00	CORNEJO CRISTIAN
244	UEAIGEC001483	MONITOR LG 18.5" LCD LED	$ 107,00	CORNEJO CRISTIAN
245	UEAIGEC001484	MONITOR LG 18.5" LCD LED	$ 107,00	CORNEJO CRISTIAN
246	UEAIGEC001485	MONITOR LG 18.5" LCD LED	$ 107,00	CORNEJO CRISTIAN
247	UEAIGEC001486	MONITOR LG 18.5" LCD LED	$ 107,00	CORNEJO CRISTIAN
248	UEAIGEC001487	MONITOR 17" SAMSUNG / LCD	$ 117,53	CORNEJO CRISTIAN
249	UEAIGEC001488	MONITOR 17" SAMSUNG / LCD	$ 117,53	CORNEJO CRISTIAN
250	UEAIGEC001489	MONITOR 17" SAMSUNG / LCD	$ 117,53	CORNEJO CRISTIAN
251	UEAIGEC001490	MONITOR 17" SAMSUNG / LCD	$ 117,53	CORNEJO CRISTIAN
252	UEAIGEC001491	MONITOR 17" SAMSUNG / LCD	$ 117,53	CORNEJO CRISTIAN
253	UEAIGEC001492	MONITOR 17" SAMSUNG / LCD	$ 117,53	CORNEJO CRISTIAN
254	UEAIGEC001493	MONITOR 17" SAMSUNG / LCD	$ 117,53	CORNEJO CRISTIAN
255	UEAIGEC001494	MONITOR 17" SAMSUNG / LCD	$ 117,53	CORNEJO CRISTIAN
256	UEAIGEC001495	MONITOR 17" SAMSUNG / LCD	$ 117,53	CORNEJO CRISTIAN
257	UEAIGEC001496	MONITOR 17" SAMSUNG / LCD	$ 117,53	CORNEJO CRISTIAN

PROYECTORES

ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
UEA0024000001	**PROYECTOR EPSON POWER LITE S12+**	$ 575,00	TAPIA CARDENAS EDGAR GONZALO
UEA0024000002	**PROYECTOR EPSON POWER LITE S12+**	$ 575,00	TAPIA CARDENAS EDGAR GONZALO
UEA0024000003	**PROYECTOR EPSON POWER LITE S12+**	$ 575,00	TAPIA CARDENAS EDGAR GONZALO
UEA0024000004	**PROYECTOR EPSON POWER LITE S12+**	$ 575,00	TAPIA CARDENAS EDGAR GONZALO
UEA0024000005	**PROYECTOR EPSON POWER LITE S12+**	$ 575,00	TAPIA CARDENAS EDGAR GONZALO
UEA0024000006	**PROYECTOR EPSON POWER LITE S12+**	$ 575,00	TAPIA CARDENAS EDGAR GONZALO
UEA0024000007	**PROYECTOR EPSON POWER LITE S12+**	$ 575,00	TAPIA CARDENAS EDGAR GONZALO
UEAIGEC001423	**PROYECTOR EPSON POWER LITE S12+**	$ 770,00	PALACIOS ESCANDON JEANNET
UEAIGEC001424	**PROYECTOR EPSON POWER LITE S12+**	$ 770,00	PALACIOS ESCANDON JEANNET
UEAIGEC001425	**PROYECTOR EPSON POWER LITE S12+**	$ 770,00	PALACIOS ESCANDON JEANNET
UEAIGEC001426	**PROYECTOR EPSON POWER LITE S12+**	$ 770,00	PALACIOS ESCANDON JEANNET
UEAIGEC001427	**PROYECTOR EPSON POWER LITE S12+**	$ 770,00	BARRERA TELLO MARIELA ANTONIETA
UEA0009000003	**PROYECTOR BENQ MS510**	$ 830,00	BARRERA TELLO MARIELA ANTONIETA
UEA0009000004	**PROYECTOR BENQ MS510**	$ 830,00	BARRERA TELLO MARIELA ANTONIETA
UEA0009000005	**PROYECTOR BENQ MS510**	$ 830,00	BARRERA TELLO MARIELA ANTONIETA
UEAIGBM001115	PROYECTOR BENQ MS 500	$ 475,00	BARRERA TELLO MARIELA ANTONIETA
UEAIGBM001116	PROYECTOR BENQ MS 500	$ 475,00	BARRERA TELLO MARIELA ANTONIETA
UEAIGBM001117	PROYECTOR BENQ MS 500	$ 475,00	BARRERA TELLO MARIELA ANTONIETA
UEAIGBM001118	PROYECTOR BENQ MS 500	$ 475,00	BARRERA TELLO MARIELA ANTONIETA
UEAIGBM001119	PROYECTOR BENQ MS 500	$ 475,00	BARRERA TELLO MARIELA ANTONIETA

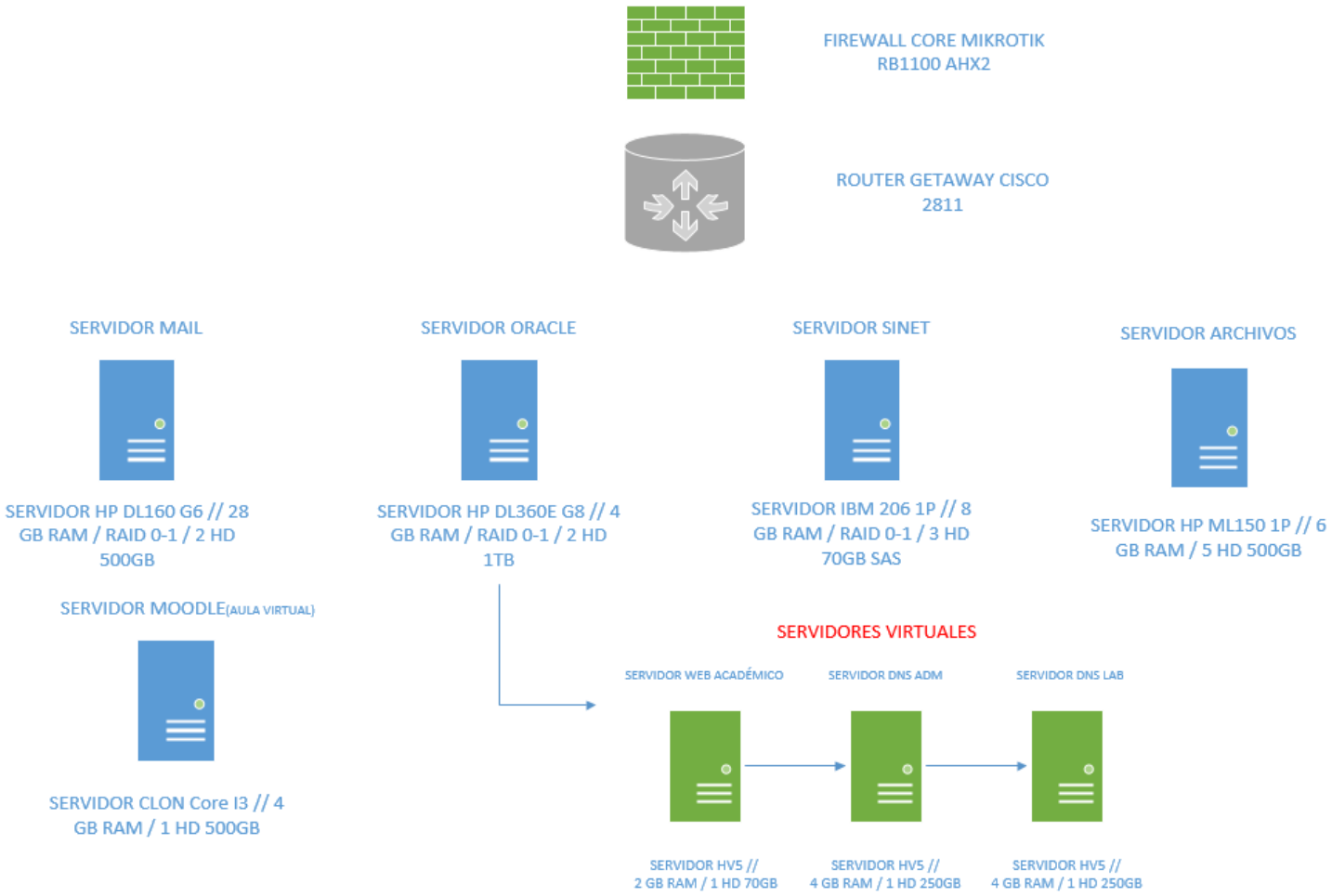
IMPRESORAS

Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
1	UEAIGEC001105	IMPRESORA SAMSUNG LASER / 2010	85,00	MONTERO ORTIZ KLEVER

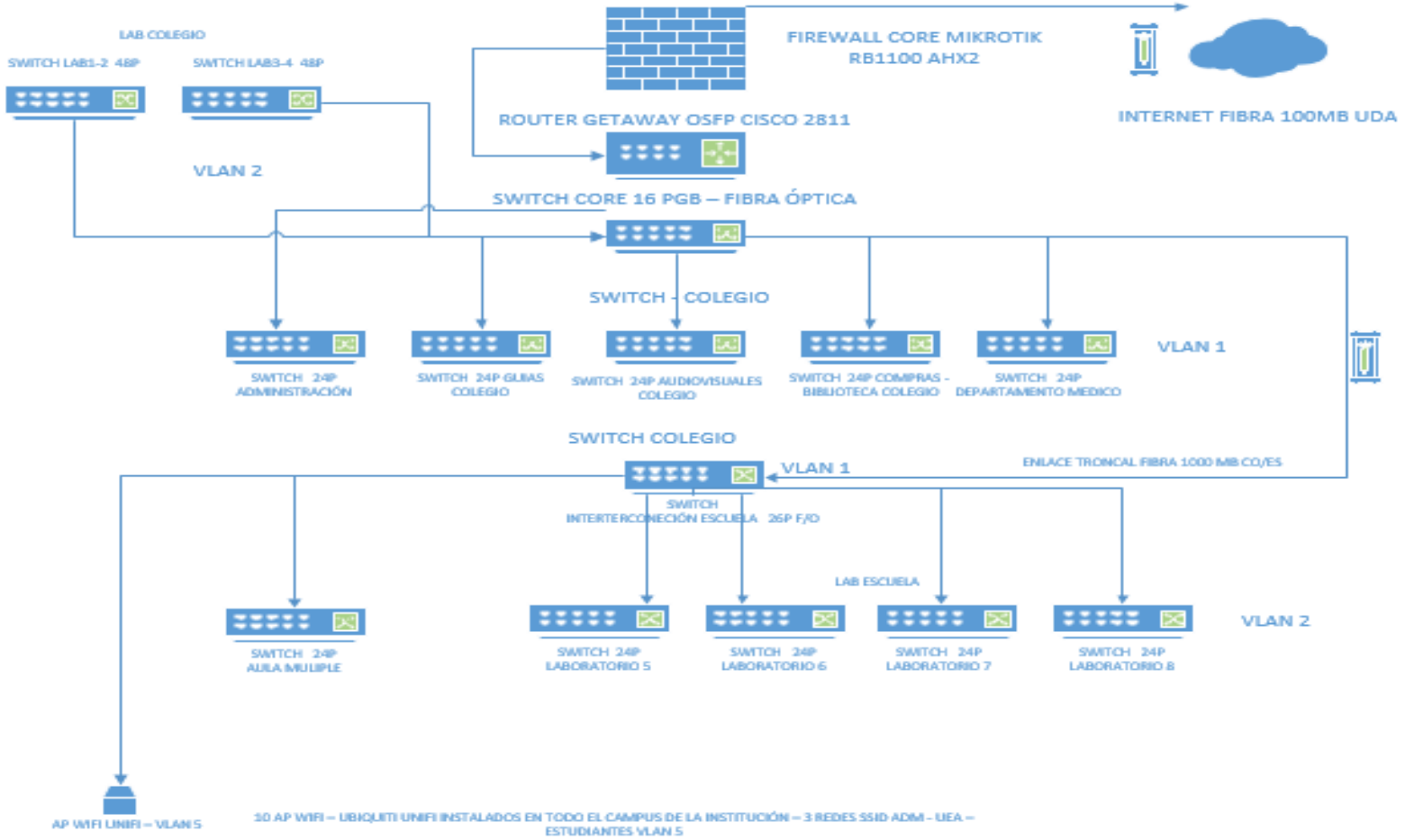
Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
2	UEAIGEC1311000004	IMPRESORA SAMSUNG LASER / ML 1915	105,00	MONTERO ORTIZ KLEVER
3	UEAIGEC001173	IMPRESORA CANON / BJC 2100	70,00	MONTERO ORTIZ KLEVER
4	UEAIGEC001403	IMPRESORA CANON MG2120	110,17	BARRERA TELLO MARIELA ANTONIETA
5	UEAIGEC001404	IMPRESORA CANON MG2120	110,17	BARRERA TELLO MARIELA ANTONIETA
6	UEAIGEC1313000002	IMPRESARA SAMSUNG / ML 4050 LASER	349,00	MONTERO ORTIZ KLEVER
7	UEAIGEC001413	IMPRESORA EPSON / L335W	241,07	BARRERA TELLO MARIELA ANTONIETA
8	UEA0027000002	IMPRESORA HP / LJ P3015-DN 128MB	690,00	TAPIA CARDENAS EDGAR GONZALO
9	UEA0028000001	IMPRESORA SAMSUNG / CLP 325 LASER COLOR	190,64	TAPIA CARDENAS EDGAR GONZALO
10	UEAIGEC001402	IMPRESORA XEROX / PHASER 3040B	57,25	BARRERA TELLO MARIELA ANTONIETA
11	UEAIGEC001412	IMPRESORA SAMSUNG / ML 2165 LASER	85,00	BARRERA TELLO MARIELA ANTONIETA
12	UEAIGEC001163	IMPRESORA SAMSUNG/ ML 1610 LASER	96,76	MONTERO ORTIZ KLEVER
13	UEAIGEC000970	IMPRESORA SAMSUNG / ML1740 LASER	145,00	SARMIENTO POLO PABLO
14	UEAIGEC000913	IMPRESORA SAMSUNG / ML1740 LASER	145,00	MONTERO ORTIZ KLEVER
15	UEAIGEC000907	IMPRESORA SAMSUNG / ML2010 LASER	200,00	MONTERO ORTIZ KLEVER
16	UEAIGEC001383	IMPRESORA SAMSUNG / ML 2240 LASER	88,99	ALVAREZ BRAVO JENNY
17	UEAIGEC001393	IMPRESORA SAMSUNG / ML 2165 LASER	85,00	BARRERA TELLO MARIELA ANTONIETA
18	UEAIGEC001390	IMPRESORA SAMSUNG / ML 2165 LASER	85,00	BARRERA TELLO MARIELA ANTONIETA
19	UEAIGEC001392	IMPRESORA SAMSUNG / ML 2165 LASER	85,00	BARRERA TELLO MARIELA ANTONIETA
20	UEAIGEC001410	IMPRESORA SAMSUNG / ML 2165 LASER	85,00	BARRERA TELLO MARIELA ANTONIETA
21	UEAIGEC001408	IMPRESORA SAMSUNG / ML 2165 LASER	85,00	BARRERA TELLO MARIELA ANTONIETA

Nº	ACTIVO	DESCRIPCION	VALOR	RESPONSABLE
22	UEAIGEC001409	IMPRESORA SAMSUNG / ML 2165 LASER	85,00	BARRERA TELLO MARIELA ANTONIETA
23	UEA0034000007	IMPRESORA SAMSUNG / ML 2165 LASER	85,00	TAPIA CARDENAS EDGAR GONZALO
24	UEA0034000006	IMPRESORA SAMSUNG / ML 2165 LASER	85,00	TAPIA CARDENAS EDGAR GONZALO
25	UEA0034000005	IMPRESORA SAMSUNG / ML 2165 LASER	85,00	TAPIA CARDENAS EDGAR GONZALO
26	UEAIGEC001389	IMPRESORA SAMSUNG / ML 2165 LASER	85,00	AUQUILLA TERAN WALTER
27	UEA0024000009	IMPRESORA SAMSUNG / ML 3312 ND	200,00	TAPIA CARDENAS EDGAR GONZALO
28	UEA0024000011	IMPRESORA SAMSUNG / ML 3312 ND	200,00	VANEGAS DELGADO DIANA VANESSA
29	UEAIGEC001374	IMPRESORA SAMSUNG / SCX-4200	200,00	TAMARIZ ESPINOZA MARIA VERONICA
30	UEA0016000001	SAMSUNG / ML 1915 LASER MONO	126,00	VANEGAS DELGADO DIANA VANESSA
31	UEAIGEC001138	IMPRESORA SAMSUNG/ ML 1610 LASER	80,00	PULLA GUERRERO MARIA PIEDAD
32	UEA0017000001	IMPRESORA SANSUNG / SCX 3200 LASER	138,00	TAPIA CARDENAS EDGAR GONZALO
33	UEA0019000006	IMPRESORA SANSUNG / SCX 3200 LASER	138,00	VANEGAS DELGADO DIANA VANESSA
34	UEA0031000002	IMPRESORA XEROX / PHASER 3040-B LASER	57,25	TAPIA CARDENAS EDGAR GONZALO
35	UEAIGEC001411	IMPRESORA XEROX / PHASER 3320 DNI LASER	399,30	BARRERA TELLO MARIELA ANTONIETA
36	UEA0031000001	IMPRESORA XEROX / PHASER 3040-B LASER	57,25	TAPIA CARDENAS EDGAR GONZALO
37	UEAIGEC001417	IMPRESORA ZEBRA / TLP-2844 TT	430,00	BARRERA TELLO MARIELA ANTONIETA
38	UEAIGBM000396	IMPRESORA XEROX / WORKCENTRE M15	845,25	SERRANO TAPIA MARCELA
39	UEAIGBM000419	IMPRESORA XEROX/ WORKCENTRE PRO M15	825,00	FAREZ LAURA

Anexo #2


FIREWALL CORE MIKROTIK
RB1100 AHX2
ROUTER GETAWAY CISCO
2811
SERVIDOR MAIL
SERVIDOR HP DL160 G6 // 28
GB RAM / RAID 0-1 / 2 HD
500GB
SERVIDOR ORACLE
SERVIDOR HP DL360E G8 // 4
GB RAM / RAID 0-1 / 2 HD
1TB
SERVIDOR SINET
SERVIDOR IBM 206 1P // 8
GB RAM / RAID 0-1 / 3 HD
70GB SAS
SERVIDOR ARCHIVOS
SERVIDOR HP ML150 1P // 6
GB RAM / 5 HD 500GB
SERVIDOR MOODLE(AULA VIRTUAL)
SERVIDOR CLON Core I3 // 4
GB RAM / 1 HD 500GB
SERVIDORES VIRTUALES
SERVIDOR WEB ACADÉMICO
SERVIDOR DNS ADM
SERVIDOR DNS LAB
SERVIDOR HV5 //
2 GB RAM / 1 HD 70GB
SERVIDOR HV5 //
4 GB RAM / 1 HD 250GB
SERVIDOR HV5 //
4 GB RAM / 1 HD 250GB

Anexo #3


LAB COLEGIO
SWITCH LAB1-2 48P
SWITCH LAB3-4 48P
VLAN 2
FIREWALL CORE MIKROTIK
RB1100 AHX2
INTERNET FIBRA 100MB UDA
ROUTER GETAWAY OSFP CISCO 2811
SWITCH CORE 16 PGB – FIBRA ÓPTICA
SWITCH - COLEGIO
SWITCH 24P ADMINISTRACIÓN
SWITCH 24P GUIAS COLEGIO
SWITCH 24P AUDIOVISUALES COLEGIO
SWITCH 24P COMPRAS - BIBLIOTECA COLEGIO
SWITCH 24P DEPARTAMENTO MEDICO
VLAN 1
SWITCH COLEGIO
VLAN 1
ENLACE TRONCAL FIBRA 1000 MB CO/ES
SWITCH INTERTERCONECIÓN ESCUELA 26P F/O
LAB ESCUELA
SWITCH 24P AULA MULIPLE
SWITCH 24P LABORATORIO 5
SWITCH 24P LABORATORIO 6
SWITCH 24P LABORATORIO 7
SWITCH 24P LABORATORIO 8
VLAN 2
AP WIFI UNIFI – VLAN 5
10 AP WIFI – UBIQUITI UNIFI INSTALADOS EN TODO EL CAMPUS DE LA INSTITUCIÓN – 3 REDES SSID ADM - UEA – ESTUDIANTES VLAN 5

Anexo #4

COMUNICADO AL RECTOR

Cuenca 12 de mayo del 2015.

Ing.
Patricio Feijoo
Unidad Educativa Particular “La Asunción”
Ciudad.

Estimado:

Me dirijo a usted con la finalidad de poner en su conocimiento, que el día 12 de mayo del 2015, daré inicio a la auditoria de la red Informática de la Unidad Educativa, previo a la elaboración de mi tesis de Ingeniero en Sistemas, sobre el tema: “Auditoria de la Gestión de Seguridad Informática de la Unidad Educativa Particular “La Asunción” basada en COBIT 5”

A la vez que le solicito informar al personal respectivo, para que me presten la ayuda y colaboración necesaria, en esta labor.

Por la atención a la presente, le anticipo mis sinceros agradecimientos,

Atentamente.

RESPUESTA RECIBIDA POR PARTE DE LA UNIDAD EDUCATIVA “LA ASUNCIÓN”

UNIDAD EDUCATIVA
LA ASUNCIÓN

Oficio No. SG-191-2015-UEA
Cuenca, 20 de mayo de 2015

Señorita
Jessica Uyaguari
Ciudad

Por medio del presente informo a usted, que cuenta con la autorización para poder dar inicio con la "Auditoria de la Gestión de Seguridad Informática", en la Unidad Educativa La Asunción

Atentamente

Master. Patricio Feijoo Calle
RECTOR (E) DE LA UNIDAD EDUCATIVA

UNIDAD EDUCATIVA PARTICULAR UNIVERSITARIA "LA ASUNCIÓN" RECTORADO CUENCA - ECUADOR

PF/fmb

PBX (593 7) 2816998 2880014
2885585 2884017 2883234
Av. 24 de Mayo 7-77 y Hernán Malo

Anexo #5

Cuenca 15 de junio del 2015.

Ing.
Patricio Feijoo
Unidad Educativa Particular “La Asunción”
Ciudad.

Estimado:

Me dirijo a usted con la finalidad de poner en su conocimiento, el informe final de Auditoría realizado en la Institución Educativa Particular “La Asunción”; en base al análisis y procedimientos aplicados a la información recopilada.

Fecha de Inicio de Auditoría:
12 de mayo del 2015.

Fecha de Redacción del informe de Auditoría:
29 de mayo del 2015.

Equipo Auditor:
Jessica Uyaguari Chalco.

Alcance de la Auditoría:

El siguiente trabajo de Auditoría aplicará COBIT como metodología para la evaluación y análisis de los diferentes procesos y controles que se aplican en el área de la tecnología de la información.

La Auditoría se centrará en el análisis de la gestión de la seguridad informática que es aplicada actualmente en la red de datos de la Institución Educativa “La Asunción”.

Se identificarán las debilidades existentes y sus riesgos potenciales, se expondrán una serie de conclusiones sobre los actuales procedimientos y controles de seguridad así como recomendaciones para el mejoramiento de la gestión de seguridad Informática.

Objetivos de la Auditoría:

Analizar y diagnosticar la actual gestión de seguridad en la red de datos de la Institución Educativa “La Asunción”.

Plantear las mejoras para la gestión de la seguridad de la red de datos.

Proponer actividades que ayudarán a identificar los controles que se requieren para garantizar la seguridad de la información.

Objetivos de Control considerados críticos

Requisitos externos de cumplimiento

Observación: No existe documentación de legislaciones y regulaciones en el área de TI de la Institución Educativa.

Riesgo: No es suficiente conocer ciertas políticas de manera verbal, en el área de TI existe regulaciones nacionales e internacionales que se deberían acoplar a la Institución educativa, tanto para la seguridad de la información existente dentro de la institución, como del hardware que se utiliza para almacenar esta información.
En caso de existir una negligencia por parte del departamento de sistemas, no existen políticas que respalden que lo realizado estuvo en contra de alguna política.
Suponiendo el cambio de personal, como es el caso de una de las integrantes del departamento de sistemas no sabe que políticas y leyes se deben cumplir dentro de la institución no es suficiente cumplir con el cargo asignado y regirse a leyes dichas de forma verbal; es necesario que todo el personal firme y conozca las legislaciones y regulaciones de la Institución educativa.

Recomendaciones: Elaborar la documentación correspondiente a las legislaciones y regulaciones del área de TI, que rijan en la Unidad Educativa; toda área de TI tiene que asegurar al usuario la confidencialidad, la integridad y/o la disponibilidad de las tecnologías de información.

Evaluación de Riesgos

Observación: No existe documentación de políticas de TI, ni de confidencialidad con respecto a los servidores y PC, y equipos de conexión de red.
Con respecto a las aplicaciones en red tanto las de escritorio como la web no guardan confidencialidad de sus cuentas y contraseñas; también estas aplicaciones no tienen todos los campos validados, esto crea inseguridad en la información proporcionada a través de las aplicaciones en red.

Riesgo: Los riesgos son los mismos con respecto a la carencia de documentación, esto no crea seguridad en el área de las tecnologías de Información.
Con respecto a las claves guardadas en la base de datos es importante cifrarlas con la finalidad de asegurar integridad de la información ya que pueden sufrir de hurto, adulteración, fraude, modificación, revelación, pérdida, sabotaje, vandalismo, crackers, hackers, falsificación, robo de contraseñas, alteraciones etc.
Con respecto a los campos no validados, es importante recordar que todos los campos son importantes no solo los de cedula y mail, el objetivo es garantizar que la

información proporcionada es confiable; en el caso del campo “nombre” se puede ingresar números o caracteres especiales esto rompería con el objetivo de contener información confiable; no se puede confiar ciegamente en el usuario ya que puede haber errores por descuido, falta de seriedad, o un ordenador intentando acceder a la información de la Institución.

Recomendaciones: Elaborar documentación de políticas que rijan el área de TI dentro de la institución, también se recomienda cifrar las claves de los usuarios *(estudiantes, padres de familia y administrativos)*. Toda área de TI tiene que asegurar al usuario la confidencialidad, la integridad y/o la disponibilidad de las tecnologías de información.

Es necesario también validar todos los campos mostrados al usuario para evitar el ingreso de información no confiable.

Por la atención a la presente, le anticipo mis sinceros agradecimientos,

Atentamente.

Jessica Uyaguari Chalco
CI. 0104985296

Anexo #6

Articulo 6301 basado en las leyes Internacionales en el área de TI de Colombia (Ministerio de Tecnologías de la Información y las Comunicaciones, 2014)

Dominio	Nombre corto	Descripción
Estrategia de TI	Entendimiento estratégico	Las entidades y el sector deben formular una estrategia de TI de la entidad y el sector respectivamente a partir del entendimiento de: • El contexto de negocio de la entidad y el sector que incluye, entre otros. • La postura estratégica de la entidad: misión, visión, principios, valores. • Los procesos que se desarrollan a nivel sectorial e institucional. • Los servicios e interacciones que el sector tiene con todas las comunidades y personas naturales y jurídicas. • El portafolio de productos y servicios que cada entidad presta. • La organización de la entidad. • El entorno normativo de la entidad y sus políticas internas. • El Plan Nacional de Desarrollo, el Plan Estratégico del Sector y el Plan Estratégico Institucional. • Las tendencias del mercado al que pertenece el sector así como las tendencias en TI. • Los planes programas y proyectos de TI que viene adelantando y su alineación con planes, programas y proyectos de la entidad. • La integración y alineación con el negocio de la entidad de: • La Arquitectura de Información. • La Arquitectura de Sistemas de Información. • La Arquitectura de Servicios Tecnológicos. • El Modelo de Operación, Gestión y Gobierno de TI. • La estrategia de Uso y Apropiación de las TI.
Estrategia de TI	Analizar FODA	La institución, deberá realizar un análisis FODA de la situación actual de TI en la entidad, para todos los dominios de la Arquitectura Empresarial AE de TI. El análisis FODA debe recibir el visto bueno de los directores de la entidad. La Institución debe asegurar la conformidad y dar el visto bueno de los directores de la entidad y de la instancia de Gobierno de TI, donde se presente este análisis de la FODA de TI.

Dominio	Nombre corto	Descripción
Estrategia de TI	Definir la Arquitectura	La AE de la entidad debe adoptar el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI, y adicionalmente debe definir, desarrollar y detallar los componentes del Marco en lo específico de la entidad. • La estrategia de desarrollo de la AE del sector debe quedar consignada en un documento llamado Estrategia de Transformación de AE Sector. • La definición de la estrategia de desarrollo de la AE de la entidad debe quedar consignada en el documento Plan de Transformación e Implementación de AE de la Entidad. • Estos planes deben ser elaborados para un período definido entre 4 y 6 años, dependiendo del tamaño de la entidad y del sector. Estos planes deben tener continuidad de manera que los cambios de Gobierno no afecten el desarrollo de la AE de la entidad.
Estrategia de TI	Implementación de la Arquitectura.	Cada entidad debe tener un plan de Transformación e implementación de su Arquitectura Empresarial de acuerdo a las iniciativas definidas en la Estrategia de Transformación de AE del sector y de la estrategia de negocio de la entidad. El Plan de Transformación e Implementación de la AE de la entidad, deberá estar alineado con la normatividad vigente, las políticas, procesos y servicios del modelo integral de gestión de la entidad.
Estrategia de TI	Mantenimiento de la Arquitectura.	Cada sector y entidad debe contar con un proceso que permita trimestralmente evaluar y mantener actualizada la AE, acorde con los cambios estratégicos, organizacionales y tecnológicos de la entidad, el sector y el entorno. Estos cambios se deben reflejar en los documentos: • Estrategia de Transformación de AE del Sector. • Plan de Transformación e Implementación de la AE de la entidad. Desde la operación continua de la entidad, cada una de ellas debe reportar trimestralmente al sector la completitud de la implementación de la AE en la entidad que permita hacerle mantenimiento a la AE.
Estrategia de TI	Evolución de la arquitectura.	La Arquitectura de la entidad y del sector debe tener una mirada prospectiva hacia la adopción de nuevas tendencias, identificación e incorporación de nuevas oportunidades y el logro de un nivel de madurez superior como consecuencia de su implementación. Desde la operación continua de la entidad, cada una de ellas debe considerar la evolución de la AE con TI, y para esto podrá generar iniciativas de evolución.

Dominio	Nombre corto	Descripción
Estrategia de TI	Portafolio de Servicios	Las entidades deben contar con un portafolio de servicios de negocio, apoyados por TI, de tal manera que el servicio atienda las necesidades de los usuarios externos e internos. Debe existir un Portafolio de Servicios de TI en el que se registre como proyectos, las iniciativas que han sido aprobadas por la instancia de gobierno de TI que se defina. Este registro debe permitir la trazabilidad de proyectos que contribuyen a evolucionar el Portafolio de Servicios de la entidad. Debe existir una correlación entre el Portafolio de Servicios de TI en la entidad y su Catálogo de Servicios de TI. El catálogo es una herramienta de gestión operativa de TI, que entre otros permite garantizar que los servicios vigentes de TI se están prestando con los acuerdos de servicio definidos con el usuario de la entidad y los terceros proveedores de esta y de TI.
Estrategia de TI	Demanda y Capacidad de servicios	Cada entidad debe identificar y estimar las capacidades y recursos requeridos para la implementación de las iniciativas TI Definición de apoyo tecnológico a los procesos. La definición de las necesidades de sistematización y apoyo tecnológico a los procesos de la entidad, deben realizarse con base en el mapa de procesos que las entidades deben implementar en el sistema de gestión de calidad.
Estrategia de TI	Recursos financieros	La Institución debe en equipo con el área de Planeación de la e entidad, asegurar una correspondencia directa entre las cifras financieras del Portafolio de Planes, Programas y Proyectos de TI; con las del Plan de Acción y de Compras de TI, y éstas con las del presupuesto destinado a gestión de TI; para lograr una mirada completa de planeación y ejecución financiera., tanto en los rubros de inversión como en los de funcionamiento.
Estrategia de TI	Iniciativas TI	• La Institución debe participar en el diseño y/o mejoramiento de los procesos de negocio de tal manera que pueda identificar iniciativas TI a incorporar en estos y que contribuyan a lograr transversalidad, coordinación, articulación, mayor eficiencia y oportunidad; menores costos, mejores servicios, menores riesgos y mayor seguridad para el negocio de la entidad. La definición de apoyo tecnológico a los procesos la organización, debe realizarse de manera alineada con el sistema de gestión de calidad de la entidad, al Plan de Transformación e implementación de la AE de la entidad, • Las iniciativas TI deberán garantizar la trazabilidad con: § Las metas de negocio § Los planes, programas y proyectos de negocio § Los procesos de negocio § Las metas de TI § El portafolio de planes, programas y proyectos de TI. Una iniciativa deja de ser iniciativa cuando la instancia de gobierno de la entidad, el sector o el país le asigne un presupuesto para su ejecución.

Dominio	Nombre corto	Descripción
Estrategia de TI	PETI	El PETI debe incluir la definición de los criterios de priorización de las iniciativas en el escenario de tiempo definido en el Plan de Transformación e Implementación de la AE de la entidad. y por consiguiente debe ser revisado y/o actualizado anualmente sin perjuicio del seguimiento que se hace a su implementación trimestralmente. Estos criterios de priorización deben ser definidos en equipo con los directivos de la entidad. El PETI es entonces la herramienta estratégica de gestión que define el norte de acción estratégico en materia de TI de la entidad.
Estrategia de TI	Definición de políticas TI, continuidad, privacidad y seguridad de la información	Cada entidad debe definir las Políticas TI para que sean aprobadas por la instancia de gobierno de TI definida por la entidad, con el fin de tener como mínimo un ambiente controlado de: • Arquitectura Empresarial para gobernar su desarrollo, implementación y mantenimiento. • Seguridad, privacidad y gestión de la información; la cual deberá incluir la implementación de un Sistema de Gestión de la Seguridad de la Información, conforme al Marco de Referencia de AE. Este sistema debe facilitar la organización, liderazgo y control sobre las decisiones de seguridad de la información, y garantizar la alineación con la normatividad vigente, las políticas, procesos y servicios del modelo integral de gestión y el modelo de gobernabilidad de la entidad, desde la definición de las necesidades, requerimientos de apoyo tecnológico y recursos, hasta la implementación de las soluciones. • Continuidad de negocio para gobernar el diseño y pruebas de los planes de continuidad y recuperación del negocio. • Sistemas de información que permitan gobernar el desarrollo e implantación de sistemas de información. • Acceso a la tecnología y uso de las facilidades por parte de los usuarios.
Estrategia de TI	Mantenimiento de políticas TI continuidad, privacidad y seguridad de la información	El sector y sus entidades deben contar con un proceso integrado que permita evaluar la aplicación y los resultados de las políticas TI, la continuidad, privacidad y seguridad de la información; de acuerdo con los cambios estratégicos, organizacionales y tecnológicos, y su replanteamiento o mejoramiento de ser necesario

Dominio	Nombre corto	Descripción
Estrategia de TI	Estrategia de Comunicación TI	Cada entidad debe definir una estrategia de gestión del cambio organizacional para asegurar la implementación de las iniciativas TI del PETI, que asegure su apropiación de todos los niveles de la organización. La estrategia de comunicación TI se debe preparar a partir del análisis de: • La postura estratégica de TI. • Los servicios de TI. • Las políticas de TI, de continuidad de negocio, de privacidad y seguridad de la información. • Las iniciativas TI documentadas en el PETI que apoyan la transformación de la AE del sector. • El plan de transformación e Implementación de la AE de la entidad. • El valor que entrega la estrategia de TI al negocio de la entidad. Adicionalmente debe contemplar: • La estrategia de comunicación. • Los tipos de mensajes a comunicar, los medios de publicación. • Los públicos a los que están dirigidos y los mecanismos de retroalimentación. • La definición de los indicadores de medición del impacto y ejecución de la estrategia de TI.
Estrategia de TI	Modelo Transición	La Institución en coordinación con las áreas de negocio de la entidad, debe diseñar e implementar un modelo de transición que garantice la estabilidad de la operación del negocio de la entidad durante la implementación y paso a producción de las iniciativas consignadas en el PETI. El modelo de transición debe estructurarse a partir de análisis de brecha de las iniciativas TI. Esto para garantizar un esquema controlado de las entregas a la operación de productos y/o servicios de TI planeados en el PETI.
Estrategia de TI	Hoja de ruta de Transformación implementación de AE de la entidad	La entidad debe definir una hoja de ruta en la que mediante grafos se pueda visualizar la evolución del Plan de Transformación e Implementación de la AE de la entidad. Esta hoja de ruta deberá ser preparada con base en las iniciativas presentadas en el PETI, y deberá ser actualizada anualmente, producto del seguimiento al PETI.
Estrategia de TI	Gobierno de la Implementación de la Estrategia de TI	Cada entidad debe implementar un proceso de gobierno de TI que facilite la evaluación, selección y priorización de iniciativas TI como respuesta a las problemáticas y necesidades de los procesos y estrategias de la entidad y del sector.
Estrategia de TI	Recursos financieros	La Institución, debe ser la responsable de formular, administrar, ejecutar y hacer seguimiento de las fichas de los proyectos de inversión requeridos para llevar a cabo la implementación de la estrategia de TI. El proceso de gestión de proyectos de inversión debe cumplir con los lineamientos que para este efecto establezca el Departamento Nacional de Planeación.

Dominio	Nombre corto	Descripción
Estrategia de TI	Portafolio de planes, programas y proyectos TIC	La entidad debe contar con un portafolio de planes, programas y proyectos de TI que permita la ejecución de las iniciativas TI definidas en el PETI. Los proyectos de TI deben diferenciar sus componentes asociados a: • Sistemas de información • Servicios tecnológicos. • Gestión de TI Al portafolio se le debe hacer seguimiento periódico acordado en el gobierno de TI, teniendo en cuenta un responsable para su gestión y actualización de avance, de tal forma que se puedan tomar acciones correctivas o de mejoramiento tendientes a cumplir con las metas estratégicas.
Estrategia de TI	Seguimiento al desempeño y cumplimiento	La Institución debe: • Realizar trimestralmente, el seguimiento a los indicadores de desempeño y cumplimiento de la estrategia de TI. El proceso de seguimiento deberá contemplar una carga mínima para los funcionarios en el reporte de información de seguimiento, que deberá apoyarse principalmente en procesos automáticos y semiautomáticos; información veraz que refleje el estado real de avance de la entidad. • Con los resultados del análisis de estos indicadores, deberá preparar un informe de análisis y definición de iniciativas de mejora a los servicios de TI. Este análisis debe realizarse por diferentes criterios como son entre otros: dominios TI, impacto en proceso de negocio y estrategias de negocio. • Tomar acciones para lograr una exitosa ejecución de los planes y proyectos de TI, definidos para la vigencia. • Realizar un seguimiento cruzado del Portafolio de Planes, Programas y Proyectos de TI; con el Plan de Acción y de Compras de TI, y éste con el presupuesto destinado a gestión de TI; para lograr una mirada completa de planeación y ejecución financiera.
Estrategia de TI	Tablero de Indicadores	La entidad debe contar con un tablero de indicadores TI, que permita tener una visión integral de los avances y resultados en el desarrollo de la Estrategia TI. El Tablero de Indicadores TI debe contemplar indicadores de: • Cumplimiento. • Impacto. • Avance según la Hoja de Ruta de AE. • Desempeño de la gestión de TI.
Gobierno de TI	Alineación	La entidad en sus instancias de relacionamiento, debe monitorear, evaluar y direccionar el cumplimiento de la propuesta de valor del portafolio de servicios de TI, y el portafolio de planes, programas y proyectos de TI. La Institución debe participar en las instancias de gobierno de la entidad, en donde se tomen decisiones relacionadas con los procesos de negocio, que incorporen soluciones y/o servicios tecnológicos, para contribuir al logro de una visión transversal, y por ende obtener la coordinación, articulación, mayor eficiencia y oportunidad con menores costos, mejores servicios, menores riesgos y mayor seguridad.

Dominio	Nombre corto	Descripción
Gobierno de TI	Compromiso de Mejora	La Institución debe incluir actividades que conduzcan a evaluar, monitorear y direccionar los procesos internos que se hayan establecido en estado de no conformidad, en el Marco de las Auditorías, de control interno y externo; lo anterior a fin de alinearse al compromiso de mejoramiento continuo de la administración pública de la entidad.
Gobierno de TI	Claridad	La entidad debe definir criterios específicos para la determinación del valor de TI. Entre otros se consideran criterios a tener en cuenta los siguientes: • Valor financiero que establece el costo - beneficio que tiene para la entidad, la implementación de la iniciativa, proyecto o servicio. • Valor tecnológico que cuantifica los niveles de incertidumbre o riesgo existente para la implementación. • Valor del negocio que cuantifica la alineación con la estrategia de la entidad.
Gobierno de TI	Seguridad de la Información	La entidad debe velar porque el modelo de gestión de seguridad de la información genere un valor agregado, representado en niveles de riesgos a un nivel aceptable y a un costo razonable. La Unidad de TIC de la entidad debe identificar los riesgos, elaborar el mapa de riesgos y gestionar los mismos, basados en el apetito del riesgo definido por el gobierno del negocio.
Gobierno de TI	Formalidad	Las políticas de TI definidas desde la estrategia deben ser emitidas y publicadas previa aprobación del gobierno de la entidad. Se publicarán como actos administrativos mediante los mecanismos normativos que disponga la entidad (decreto, resolución, circular o guía).
Gobierno de TI	Cumplimiento	El Gobierno de TI identificará y velará para que la normatividad externa que se debe tener en cuenta en la proporción de servicios y soluciones de TI, se cumpla.
Gobierno de TI	Liderazgo	La Unidad de Gestión de Información y las Tecnologías de Información deberá liderar el proceso de planeación, ejecución y seguimiento de los planes, programas y proyectos que correspondan al ámbito tecnológico e involucren TI. En aquellos casos en los que los planes, programas y proyectos respondan a objetivos funcionales de negocio y sean liderados por otras áreas, la Unidad deberá liderar la definición conceptual y técnica para que se asegure que la tecnología apoya correctamente la solución planteada para el negocio.

Dominio	Nombre corto	Descripción
Gobierno de TI	Planeación, ejecución y seguimiento	En todos los proyectos de TI se debe evaluar, direccionar y monitorear como mínimo, las siguientes áreas de conocimiento de los proyectos: 1. Alcance. 2. Costos. 3. Tiempo. 4. Equipo humano. 5. Compras. 6. Calidad. 7. Comunicación. 8. Manejo de los interesados. 9. Integración. Los proyectos deberán tener una relación directa con el portafolio, planes y programas definidos en la entidad y el sector. Durante la ejecución del proyecto, se deben generar espacios de transferencia de conocimiento, que faciliten el entendimiento y la futura operación de los productos y servicios intermedios y finales que serán generados.
Gobierno de TI	Indicadores de gestión de los proyectos	Para establecer el avance y la ejecución normal de los proyectos, se debe contar con un conjunto de indicadores que permitan registrar y monitorear el estado de los mismos. Se deben definir los indicadores estrictamente necesarios y suficientes, a fin de medir el avance de los entregables, el gasto que se ha causado, el valor ganado y los resultados obtenidos. De esta manera se adelantará el proceso de control que permita medir la eficiencia y la efectividad del proyecto.
Gobierno de TI	Oficina de Proyectos	En los casos en los que el volumen e importancia de proyectos así lo amerite, se debe establecer una oficina de Proyectos (en la entidad o sector), que le permita a la entidad contar con un modelo de gobierno centralizado de proyectos y proporcionar funciones de apoyo, control y dirección que generen el respectivo seguimiento y optimización de los recursos y capacidades.
Gobierno de TI	Definición de la cadena de valor de TIC	La entidad debe incluir en su cadena de valor un macroproceso para la gestión de Tecnología y Sistemas de Información, que genere mérito a la entidad y en el cual se incorporen como mínimo los procesos reglamentados por el Decreto por el cual se crea el Sistema de Gestión de Información y las Tecnologías de la Información. En la especificación del macroproceso se debe tener la definición de los procedimientos, resultados, indicadores y mecanismos de control; para garantizar que se desarrolle normalmente la función según los criterios de calidad.

Dominio	Nombre corto	Descripción
Gobierno de TI	Implementación de los procesos de TIC:	La Unidad de Gestión de Información y las Tecnologías de la Información tiene la responsabilidad de implementar su modelo de organización y de operación. A partir de las definiciones hechas en la estrategia, se debe incluir como mínimo los siguientes procesos: • Planeación y Dirección. Corresponde al desarrollo de actividades tendientes a la definición de las políticas, objetivos y metas a alcanzar durante los períodos legales correspondientes para la gestión estratégica de la información y de las tecnologías de la información. • Gestión de la Información. Corresponde al desarrollo de las actividades tendientes a colectar, almacenar, analizar y explotar la información a fin de apoyar el proceso de la toma de decisiones, divulgar y proteger la información misional de cada entidad, así como la seguridad y privacidad de la información. • Gestión de TI. Implica el desarrollo de las actividades para el aprovechamiento de las Tecnologías de la Información, de tal manera que permitan cumplir con la misión de cada entidad. • Seguimiento y Control. Implica el desarrollo de actividades tendientes a la verificación y seguimiento a la gestión de la información y de las Tecnologías de Información, facilitando la realimentación continua al desempeño, resultados e impactos producidos por las actividades, la toma de decisiones y la reorientación de las acciones para garantizar el logro de los resultados previstos. Los procesos definidos deben cubrir de manera transversal las actividades relacionadas con: • Gestión del Modelo de Seguridad de la Información que garantice el cumplimiento y logro de sus objetivos y su mejora continua. • Mejoramiento continuo de los servicios de TI. • Optimización del riesgo. Teniendo en cuenta el Sistema de Gestión de Calidad de la entidad, se deberá definir las cargas de trabajo, las responsabilidades, los roles, los mecanismos de seguimiento y adelantar las capacitaciones y actividades de entrenamiento y divulgación necesarias para la apropiación de los procesos al interior del área y en la entidad.
Gobierno de TI	Evaluación de gestión TIC	En virtud de lo establecido dentro del Modelo Integral de Gestión de la Entidad, debe realizar el monitoreo y evaluación de desempeño de la gestión, a partir de las mediciones de los indicadores del macroproceso y de los acuerdos de niveles de servicio. Se debe también, determinar el nivel de avance y cumplimiento de los procesos, estableciendo oportunidades y acciones de mejoramiento. Se deberá monitorear el cumplimiento de las metas establecidas en el PETI de la entidad.
Gobierno de TI	Mejoramiento continuo TIC.	Como parte del ciclo de mejoramiento de la calidad del Sistema de Gestión de Información y las Tecnologías de la Información, la entidad deberá buscar su mejoramiento en el cumplimiento de las metas y en un mayor control de los indicadores de desempeño de los procesos y de su impacto y cubrimiento de la estrategia de TI.
Gobierno de TI	Definición de capacidades	Cada entidad debe definir, direccionar, evaluar y monitorear los recursos y capacidades necesarias y suficientes para prestar los servicios de TI, mediante los cuales se implementa la estrategia de TI. • Los recursos se deberán definir en términos de servicios tecnológicos, sistemas de información, personal y recursos financieros. • Las capacidades deben estar definidas en términos de organización, conocimiento y procesos.

Dominio	Nombre corto	Descripción
Gobierno de TI	Responsable	El responsable de la Institución debe estar en capacidad de: • Proveer la visión tecnológica y el liderazgo para desarrollar e implementar todas las iniciativas de TI definidas en la estrategia. • Es patrocinador de la AE y es quien debe lograr el compromiso de todos los interesados de la entidad, para desarrollarla (esto mientras que el concepto y la importancia no se encuentren arraigados en la entidad, momento en el cual la Alta Gerencia será quien tome el rol). • Lidera el desarrollo de la AE, apoyado en los lineamientos del Marco de Referencia. • Tiene presencia en las instancias de relacionamiento y toma de decisiones a fin de impulsar su desarrollo.
Gobierno de TI	Definición de perfiles	Los perfiles y habilidades requeridos para el personal de TI, se deben establecer en función de los procesos definidos en el macroproceso de TI. La estructura de organización de TI en caso de ser requerido, debe contemplar los equipos de recursos técnicos especializados de terceros, e incorporarlos en la gestión de los procesos y gobernabilidad de TI.
Gobierno de TI	Gestión de proveedores de TI	Todos los proveedores y contratos para el desarrollo de las iniciativas de TI deben ser administrados por la Institución. Durante el proceso pre-contractual se debe establecer un esquema claro de direccionamiento, supervisión, seguimiento y control.
Gobierno de TI	Alineación de proveedores	La Institución, debe dar a conocer a los proveedores las iniciativas de la Estrategia de TI, la contribución al negocio y el rol de su participación en la implementación de las mismas.
Gobierno de TI	Traspaso de Información	La Institución debe identificar los momentos y/o puntos en donde es necesario generar dinámicas de traspaso de información de los proveedores, a fin de garantizar la permanencia de conocimiento en la entidad.
Servicios Tecnológicos	Aplicar mejores prácticas para infraestructura tecnológica	La entidad debe definir un Plan de Arquitectura de Servicios Tecnológicos que, con foco en la capa física, incorpore las características técnicas de los elementos necesarios para cubrir la demanda tecnológica actual de la entidad así como los requerimientos proyectados a futuro de los sistemas de información y los servicios de la entidad. Este Plan debe derivar en un Diseño de Arquitectura de Servicios Tecnológicos y debe tener en cuenta acciones de mantenimiento periódico.

Dominio	Nombre corto	Descripción
Servicios Tecnológicos	Disposición de un centro de servicios tecnológicos	La entidad debe contar con un Centro de Servicios Tecnológicos por medio del cual se gestione: • La iniciativas tecnológicas de la entidad de acuerdo al Plan de Arquitectura de Servicios Tecnológicos • Las estrategias tecnológicas para que sean rentables y de calidad. • La innovación tecnológica. • Los requerimientos de Capacidad, Disponibilidad y Adaptabilidad, Estandarización de los servicios tecnológicos. • La adquisición y/o re-utilización de la tecnología requerida por la entidad de acuerdo con principios de Racionalización y Optimización. • La administración y operación de los servicios tecnológicos. Los anteriores deben cubrir las características de conectividad, software base, infraestructura, plataformas y aplicaciones; considerando las modalidades de prestación de servicios tecnológicos On Premise y On Demand.
Servicios Tecnológicos	Intercambio de Información	La entidad debe incluir dentro de su Arquitectura de Servicios Tecnológicos los elementos necesarios para realizar el intercambio de información entre las áreas de la entidad, las entidades externas del nivel sectorial y del nivel nacional. La estrategia de intercambio debe ser identificada, analizada, diseñada e implementada considerando las necesidades de interoperabilidad actuales y proyectadas a futuro, tomando en cuenta la Plataforma de Interoperabilidad disponible en el Estado colombiano.
Servicios Tecnológicos	Continuidad y disponibilidad de servicios tecnológicos	La infraestructura tecnológica debe contar con sistemas de alimentación eléctrica, mecanismos de refrigeración, soluciones de detección de incendios, sistemas de control de acceso, y sistemas de monitorización de componentes físicos que asegure la continuidad y disponibilidad del servicio así como la capacidad de atención y resolución de incidentes.
Servicios Tecnológicos	Monitoreo de la seguridad de los Servicios Tecnológicos	La entidad debe contar con herramientas de administración de seguridad para implementar, mantener, controlar y monitorear elementos de seguridad que incluya perfiles del usuario, privilegios, grupos de usuarios y sus recursos, redes, tanto a nivel interno como externo. Las herramientas deben registrar como mínimo los intentos de ingreso, las modificaciones de los privilegios, las creaciones de nuevos perfiles, usuarios y localización desde la cual se realiza el evento.
Servicios Tecnológicos	Definición y Seguimiento de Acuerdos de Nivel de Servicio	La entidad debe definir y realizar el seguimiento de los Acuerdos de Niveles de Servicio (ANS) para los servicios tecnológicos (incluyendo aquellos soportados por terceros), con el fin de cumplir sus Criterios de Calidad (ver Características de Calidad de Servicios Tecnológicos). Cada entidad deberá determinar cuál es el nivel de calidad mínimo requerido (ver Especificación Técnica).
Servicios Tecnológicos	Acceso a servicios en la nube	La entidad debe evaluar la prestación de sus servicios tecnológicos a través de la nube pública privada o hibrida según sea el caso para atender a los usuarios, entidades y ciudadanos que requieran de los servicios.

Dominio	Nombre corto	Descripción
Servicios Tecnológicos	Control del Consumo de los recursos compartidos por Servicios Tecnológicos	La entidad debe identificar, monitorear y controlar el nivel de consumo de los recursos críticos que son compartidos por los servicios tecnológicos y administrar su disponibilidad en consecuencia.
Servicios Tecnológicos	Alta disponibilidad de servicios tecnológicos	La entidad debe implementar capacidades de alta disponibilidad que incluyan balanceo de carga y redundancia para los servicios tecnológicos que estén involucrados en la continuidad del servicio de entidad, las cuales deben ser puestas a prueba periódicamente.
Servicios Tecnológicos	Reusabilidad a través de un Catálogo de Servicios Tecnológicos	La entidad debe contar con un catálogo de su infraestructura tecnológica para validar la posibilidad de implementar y reutilizar los servicios existentes considerando las necesidades actuales de las áreas de negocio y sistemas de información de la entidad. El catalogo debe contar con la información licencias, versiones, cantidades, capacidades, restricciones y las demás necesarias para decidir la viabilidad de reutilizarla o adquirir un nuevo servicio tecnológico.
Servicios Tecnológicos	Proceso de copias de seguridad y restauración	La entidad debe contar con un proceso periódico de respaldo de la configuración de sus servicios tecnológicos así como de la información almacenada en la infraestructura tecnológica. Este proceso debe ser probado periódicamente (en diferentes niveles de agregación) y debe permitir la recuperación íntegra de los servicios tecnológicos.
Servicios Tecnológicos	Gestión preventiva de los Servicios Tecnológicos	La infraestructura que soporta los servicios tecnológicos de la entidad deben contar con mecanismos de monitoreo para generar alertas tempranas ligadas los umbrales de operación que tenga definidos. En aquellos casos en los que las alertas representan la interrupción de un servicio, esta debe ser notificada a los usuarios afectados.
Servicios Tecnológicos	Análisis de vulnerabilidades	La entidad debe definir un proceso homologado y de ejecución periódica para el análisis de vulnerabilidades de la infraestructura tecnológica a través de un Plan de Pruebas que permita identificar y mitigar las brechas que puedan comprometer la seguridad de la información o puedan afectar la prestación de un servicio.
Servicios Tecnológicos	Mesa de ayuda única	La entidad debe definir el procedimiento para atender los requerimientos de soporte de primer, segundo y tercer nivel para sus servicios tecnológicos a través de una mesa de ayuda única.
Servicios Tecnológicos	Planes de mantenimiento	La entidad debe contar con un Plan de Mantenimiento Preventivo sobre toda la infraestructura y sus servicios tecnológico para asegurar una operación estable de los servicios. Este plan debe contar como mínimo con información de periodicidad, prerrequisitos, condiciones técnicas y verificaciones necesarias para asegurar el cumplimiento de los resultados de los mantenimientos preventivos.
Sistemas de Información	Definición Estratégica de los SIS-INF	Las entidades deben, en la Arquitectura de cada uno de sus SIS-INF, en primer lugar plantear una Arquitectura del Sistema de Información que aborde los diferentes dominios del Marco de Referencia de AE. A partir de esta arquitectura, debe establecer la Arquitectura de Solución que defina los diferentes componentes software que la implementan. Esta Arquitectura de Solución debe estar basada en una Arquitectura de Referencia.

Dominio	Nombre corto	Descripción
Sistemas de Información	Hoja de Ruta de SIS-INF	Las entidades deben contar, para todas las soluciones de software de sus Sistemas de Información, con una Hoja de Ruta que permita establecer un plan de mantenimiento, soporte y evolución hasta su potencial reemplazo u obsolescencia, considerando tanto los aspectos normativos que los regulan la vigencia de sus soportes tecnológicos, así como los cambios de estrategia y modelo operativo de la entidad.
Sistemas de Información	Metodología de Referencia para desarrollo de SIS-INF	La entidad debe contar con una Metodología de Referencia que defina los componentes principales de un Proceso de Desarrollo del Software que considere sus fases o etapas (ciclo de vida), las actividades principales y de soporte involucradas (ej. Gestión de la Configuración, Gestión de la Calidad, entre otros), roles y responsabilidades así como herramientas de apoyo al ciclo de vida. Esta metodología de referencia debe dar cobertura a todos las soluciones de software de los SIS-INF que la entidad construya o adapte, independientemente de su tecnología. Así mismo, debe ser común a nivel sectorial y es responsabilidad de la entidad cabeza de sector conseguir los acuerdos necesarios para ello. Esta metodología debe incorporar mejores prácticas de las metodologías de la industria, incluyendo el uso de métodos ágiles.
Sistemas de Información	Directorio de SIS-INF	La entidad debe habilitar un directorio con los SIS-INF de que dispone. Este directorio debe estar clasificado teniendo en cuenta categoría, temática y tipo de SIS-INF (incluyendo si es de infraestructura crítica). Cada SIS-INF debe incluir una descripción, si es el sistema es de interés de la entidad, sectorial o de interés nacional, la vigencia, canales de acceso, roles de acceso así como operaciones permitidas a través de una Guía de Uso del SIS-INF disponible en el propio directorio. La entidad es responsable de definir el nivel de acceso de este directorio teniendo en cuenta la normatividad asociada. Este directorio se consolida, a nivel sectorial, a través de la cabeza de sector, como un Directorio de SIS-INF sectorial. Este Directorio debe permitir realizar un análisis de reutilización ante la necesidad de construir o adquirir un nuevo sistema de información por parte de una entidad.
Sistemas de Información	Licencia abierta de uso de los SIS-INF	Aquellos elementos de software de los SIS-INF de interés sectorial o nacional deben tener una licencia de uso abierta para entidades del Estado colombiano. Esta licencia establece que la entidad debe habilitar las capacidades necesarias para que los elementos de software puedan ser prestados como servicio o cedidos a otras entidades, así mismo, establece que en aquellos casos donde las entidades realicen adaptaciones o mejoras de los elementos de software que también sean de interés sectorial o nacional, estas son responsables de distribuirlas a la entidad cabeza de sector y/o a la entidad desarrolladora del componente referido.
Sistemas de Información	Activos de Arquitectura de Referencia de los SIS-INF	La entidad debe contar con componentes de software reutilizables que hagan parte de sus Arquitecturas de Referencia tales como: Componentes de autenticación y autorización única a través de un Servicio de Directorio, de trazabilidad de la ejecución, de registro de errores, de acceso a la capa de datos, de gestión de la integridad transaccional, entre otros. La entidad deben asegurar el uso de estos componentes en sus SIS-INF.

Dominio	Nombre corto	Descripción
Sistemas de Información	Guía de Estilo y Usabilidad de los SIS-INF	La entidad debe contar con una Guía de Estilo y Usabilidad única que establezca los principios para el estilo de los componentes de presentación, estructura para la visualización de la información, procesos de navegación entre pantallas, entre otros. Esta Guía de Estilo y Usabilidad debe estar particularizada por cada medio tecnológico o canal utilizado por los SIS-INF, y así mismo debe estar alineada con los principios de Usabilidad definidos por el Estado colombiano. La entidad debe asegurarse de la aplicación de esta Guía en todos sus SIS-INF, y es la UGITI la responsable de coordinar su elaboración.
Sistemas de Información	Ambientes para los SIS-INF	La entidad debe contar con una línea de producción para sus SIS-INF con diferentes ambientes que puedan alinearse con actividades o etapas del ciclo de vida establecidas por el Proceso de Desarrollo de Software (ej. Desarrollo, Integración, Pruebas, Aceptación de Usuario o de Certificación, Capacitación, Puesta en Producción, entre otros).
Sistemas de Información	Arquitecturas de Referencia de SIS-INF	Las entidades deben contar con Arquitecturas de Referencia, por medio de la cuales se establezcan aquellos patrones de diseño, mejores prácticas tecnológicas, recomendaciones de desarrollo, herramientas especificas de apoyo a la construcción así como componentes tecnológicos reutilizables que aseguren el diseño de cualquier Arquitectura de Solución de manera eficiente, homogénea y de calidad. La UGITI es la unidad responsable de definir y evolucionar estas Arquitecturas de Referencia.
Sistemas de Información	Arquitecturas de Solución de SIS-INF	La entidad debe contar, para las soluciones software de sus SIS-INF, con una diseño de Arquitectura de Solución que, vigente a través de las etapas del ciclo de vida e incluya la definición de vistas de contexto, funcional, de despliegue y de información para representar todos sus componentes, principios y patrones de diseño así como actores involucrados.
Sistemas de Información	Implementación de COM-INF a través de SIS-INF	Los SIS-INF de la entidad deben soportar la Arquitectura de los COM-INF definida, considerando la Taxonomía, el Diccionario de Datos establecido, el Catálogo de Flujos de Información, el Directorio de Servicios así como las necesidades de Análisis y Toma de Decisiones de los COM-INF.
Sistemas de Información	Apertura de Datos en los SIS-INF	La entidad debe habilitar en sus SIS-INF aquellas características técnicas, funcionales y no funcionales necesarias para la apertura de sus datos de acuerdo a la normativa del Estado colombiano. Estas características deben permitir que la apertura se realice de un mismo modo tanto hacia el Portal de Datos de Abiertos del Estado colombiano como hacia portales propios de la entidad.
Sistemas de Información	Interoperabilidad de SIS-INF	La entidad debe habilitar en sus SIS-INF aquellas características técnicas, funcionales y no funcionales necesarias para interactuar con la Plataforma de Interoperabilidad del Estado colombiano, partiendo para ello del Catálogo de Flujos de Información y las necesidades de intercambio de información con otras entidades que de este se derivan.

Dominio	Nombre corto	Descripción
Sistemas de Información	Plan de Pruebas de los SIS-INF	La entidad debe contar con un Plan de Pruebas en la construcción de los componentes software de su SIS-INF que incluya etapas para pruebas unitarias, de integración, de aceptación de usuario, de rendimiento y estrés, de despliegue y de seguridad. La aceptación de cada una de las etapas del Plan de Pruebas debe estar vinculada a la transición del Sistema de Información a través de los diferentes ambientes. Este Plan de Pruebas debe formar parte del Proceso de Desarrollo de Software.
Sistemas de Información	Servicios de Mantenimiento de SIS-INF	La entidad debe establecer Acuerdos de Nivel de Servicio para sus servicios de mantenimiento de SIS-INF establecidos con terceros. Estos debe tener en cuenta las etapas de transición, prestación y devolución del mismo para asegurar la continuidad de los SIS-INF involucrados.
Sistemas de Información	Actualización y requerimientos de cambio de los SIS-INF	La entidad, en los servicios de soporte de sus SIS-INF, debe formalizar la petición de nuevas funcionalidades o de cambios a las existentes a través de un procedimiento de Gestión de Solicitudes de Cambio.
Sistemas de Información	Análisis de Impacto de SIS-INF	La entidad debe disponer de mecanismos para realizar análisis de impacto ante un cambio o modificación de alguno de los componentes de software de sus SIS-INF.
Sistemas de Información	Plan de Capacitación y Entrenamiento de los SIS-INF	La entidad debe contar, para cada SIS-INF, con un Plan de Capacitación y Entrenamiento que facilite el uso y apropiación durante todo el ciclo de vida del sistema. La entidad debe considerar para la ejecución del plan los métodos más adecuados según las características del SIS-INF (ej. autoformación, guías, sesiones presenciales, formación a formadores, entre otros).
Sistemas de Información	Manual de Usuario, Técnico y de Operación de SIS-INF	La entidad debe asegurar que todos sus SIS-INF, en su etapa de entrega, cuenten con un Manual de Usuario, un Manual Técnico y un Manual de Operación vigentes que asegure la transferencia de conocimiento para el uso del sistema hacia los usuarios, hacia la UGITI, y hacia servicios de soporte tecnológico, respectivamente.
Sistemas de Información	Plan de Calidad de los SIS-INF	La entidad debe contar con un Plan de Calidad de los componentes software de sus SIS-INF que incluya etapas de aseguramiento, control e inspección y tenga en cuenta tanto actividades de medición de indicadores de calidad (a través de un Tablero de Control) como actividades preventivas, correctivas y de mejoramiento tanto en ámbitos técnicos, funcionales y no funcionales. Este Plan de Calidad debe formar parte del Proceso de Desarrollo de Software.
Sistemas de Información	Criterios no funcionales y de calidad de los SIS-INF	La entidad debe asegurar que el diseño de sus SIS-INF cumple con los Criterios No Funcionales y de Calidad definidos, incluyendo Escalabilidad, Interoperabilidad, Multicanalidad, Funcionalidad, Fiabilidad, Usabilidad, Eficiencia, Mantenibilidad y Portabilidad.
Sistemas de Información	Seguridad y Privacidad de los SIS-INF	La entidad debe incorporar, en el diseño de sus SIS-INF, aquellos componentes de seguridad alineados con la normativa establecida que incluyan, como mínimo: el tratamiento de la privacidad de la información, la implementación de controles de acceso (autorización y autenticación) así como los mecanismos de integridad y cifrado de la información.
Sistemas de Información	Auditoría y trazabilidad de SIS-INF	Las entidad deben incluir, en el diseño de sus Sistemas de Información, mecanismos que aseguren el registro histórico para la trazabilidad de las acciones realizadas por los usuarios. Por cada acción, el registro debe incluir la fecha y hora, el usuario y la acción o evento involucrado.

Dominio	Nombre corto	Descripción
Uso y Apropiación	Identificación de stakeholders	La estrategia de uso y apropiación está basada principalmente por los grupos de interés , los cuales deben ser identificados, priorizados, categorizados y clasificados. Se deben tener en cuenta los diferentes públicos involucrados por la oferta de sistemas y servicios de información
Uso y Apropiación	Involucramiento en cascada	El involucramiento de los grupos de interés debe ser convocado desde la Alta Dirección en cascada hacia el resto de los niveles organizacionales.
Uso y Apropiación	Liderazgo visible	La Alta Dirección debe ser modelo a seguir en el uso y apropiación de las TI en las organizaciones.
Uso y Apropiación	Visión compartida	Las entidades podrán impulsar el compromiso hacia la adopción y uso de las TI mediante el alineamiento y el desarrollo de una identidad común con los propósitos estratégicos de la gestión de TI. De esta manera se establecen vínculos comunes que conllevan al compromiso.
Uso y Apropiación	Plan de Formación	El desarrollo de capacidades en TI debe hacer parte del plan de formación de la Entidad
Uso y Apropiación	Toma de decisiones	Las competencias en TI deben generar un entorno de conocimiento para la toma de decisiones de la Entidad.
Uso y Apropiación	Prácticas TI	La cultura organizacional de la Entidad debe reflejar buenas prácticas de TI.
Uso y Apropiación	Lógicas del cambio	La Entidad debe analizar sus propias lógicas de cambio y gestionar los impactos priorizando su nivel, de manera anticipada.
Uso y Apropiación	Herramientas de cambio	La Entidad debe desarrollar herramientas gerenciales y de aprendizaje que apalanquen el uso y la apropiación de las TI.
Uso y Apropiación	Dotación y acceso	Las entidades deben asegurar el uso y la apropiación de los sistemas de información y servicios tecnológicos desde la identificación de iniciativas estratégicas de TI para el negocio, hasta facilitar la dotación de tecnología y fomentar su acceso.
Uso y Apropiación	Cultura TI	La Entidad debe diseñar, aplicar y monitorear indicadores de impacto del uso y apropiación de las TI alineados a los de la cultura organizacional.
Uso y Apropiación	Sostenibilidad del cambio	Las iniciativas de TI se enmarcan en una estrategia de transformación que le dé continuidad de largo plazo en la entidad, superando estadios de estabilización hasta apropiar las TI como parte de las prácticas organizacionales.
Uso y Apropiación	Adopción de TI	Los indicadores de Uso y Apropiación deben evaluar el nivel de adopción de tecnología y la satisfacción en el uso.

Referencias

A, V. (2012). *Análisis de Riesgo.*

COBIT 5. (2000). *Comite directivo de COBIT y IT Governance Institute.*

COBIT 5. (2012). *Enabling Processes.*

COBIT. (s.f.). *Directrices de auditoria III.*

Gobernance Institute (IT). (2007). *COBIT 4.1.*

Herrera, J. (s.f.). *Administracion de Redes.*

ISACA. (2012). *COBIT 5 (ESPAÑOL).* Obtenido de https://cobitonline.isaca.org/

ISACA. (2014). Obtenido de http://www.isaca.org/about-isaca/history/espanol/pages/default.aspx

ISACA. (2014). *TRUST IN, AND VALUE FROM, INFORMATION SYSTEMS.* Obtenido de www.isaca.org/COBIT/Documents/

Ley Organica de educacion Superior. (2010). *Consejo de Educacion Superior (CES).* Obtenido de http://www.ces.gob.ec/descargas/ley-organica-de-educacion-superior

Mifsud, E. (2012). *Introducción a la seguridad informática - Políticas de seguridad*. Obtenido de http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=4

Ministerio de Tecnologías de la Información y las Comunicaciones. (2014). *MITIC*. Obtenido de http://www.mintic.gov.co/portal/604/w3-channel.html

Orozco, P. (s.f.). *Gestión de la Red 3.*

TELECOMUNICACIONES IV. (s.f.). *SISTEMA DE GESTIÓN DE REDES Y SERVICIOS DE TELECOMUNICACIONES.*

Doctora Jenny Ríos Coello, Secretaria de la Facultad de Ciencias de la Administración de la Universidad del Azuay,

C E R T I F I C A:

Que, el H. Consejo de Facultad en sesión realizada el 08 de enero del 2015 conoció la petición de la estudiante **Jéssica Paola Uyaguari Chalco** con código 45785, que denuncian su trabajo de titulación (tesis) "AUDITORIA DE LA GESTION DE SEGURIDAD INFORMATICA DE LA UNIDAD EDUCATIVA PARTICULAR LA ASUNCION BASADA EN COBIT 5", previa a la obtención del Grado de Ingeniero de Sistemas y Telemática. El Consejo de Facultad acoge el informe de la Junta Académica y aprueba la denuncia de tesis. Designa como Director al ingeniero Esteban Crespo Martínez y como miembros del Tribunal Examinador a los ingenieros Juan Córdova Ochoa y Rubén Ortega López. De conformidad a la disposición general tercera del Reglamento de Régimen Académico, la peticionaria tiene un plazo equivalente a dos períodos académicos (semestres) para desarrollar y terminar su trabajo de titulación, esto es hasta el **8 de enero de 2016**.

Cuenca, enero 9 de 2015

C O N V O C A T O R I A

Por disposición de la Junta Académica de Ingeniería de Sistemas y Telemática **CONVOCO** a los Miembros del Tribunal Examinador a la sustentación del Protocolo del Trabajo de Titulación denominado: **"AUDITORIA DE LA GESTION DE SEGURIDAD INFORMATICA DE LA UNIDAD EDUCATIVA PARTICULAR LA ASUNCION BASADA EN COBIT 5"** presentado por la señorita **JESSICA PAOLA UYAGUARI CHALCO** (45785) previa a la obtención del grado de Ingeniera de Sistemas, para el día **JUEVES 6 DE NOVIEMBRE DE 2014, a las 18H30**

Cuenca, 30 de octubre de 2014

Dr. Romel Machado Clavijo
Secretario de la Facultad

Ing. Esteban Crespo M.

Ing. Juan Córdova O.

Ing. Rubén Ortega L.

Comunicado

Oficio Nro. 126-2014-DIST-UDA

Cuenca, 28 de Octubre de 2014

Señor Ingeniero
Xavier Ortega Vázquez
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMNISTRACIÓN
Presente.-

De nuestras consideraciones:

La Junta Académica de la Escuela de Ingeniería de Sistemas y Telemática, reunida el día 28 de Octubre del 2014, recibió el proyecto de tesis titulado "Auditoría de la gestión de seguridad informática de la Unidad Educativa Particular La Asunción basada en COBIT 5", presentada por la estudiante Jessica Uyaguari Chalco, estudiante de la Escuela de Ingeniería de Sistemas y Sistemas y revisado por el Ing. Esteban Crespo previo a la obtención del título de Ingeniero de Sistemas y Telemática.

La Junta solicita por su digno intermedio notificar al tribunal designado y determinar lugar, fecha y hora de sustentación.

Por lo expuesto, y de conformidad con el Reglamento de Graduación de la Facultad, recomienda como director y responsable de aplicar cualquier modificación al diseño del trabajo de graduación posterior a al Ing. Esteban Crespo y como miembros del Tribunal al Ing. Juan Córdova y Ing. Rubén Ortega.

Atentamente,

Ing. Marcos Orellana Cordero
Director Escuela de Ingeniería de Sistemas y Telemática
Universidad del Azuay

Sustentación del Diseño de Tesis (Doctor Romel Machado Clavijo)

Fecha: 31-10-2014

ESCUELA DE INGENIERIA DE SISTEMAS

Diseños de Tesis
Escuela de Sistemas
Estudiante: Jessica Uyaguari Chalco con código 45785.
Tema: "AUDITORIA DE LA GESTION DE SEGURIDAD INFORMATICA DE LA UNIDAD EDUCATIVA PARTICULAR LA ASUNCION BASADA EN COBIT 5"
Para: La obtención del título de Ingeniera en Sistemas
Director: Ing. Esteban Crespo
Tribunal: Ing. Juan Córdova
Tribunal: Ing. Rubén Ortega.

DIA:

FECHA:

HORA:

ACTA

SUSTENTACIÓN DE PROTOCOLO/DENUNCIA DEL TRABAJO DE TITULACIÓN

1.1.1. **Nombre del estudiante:** JESSICA PAOLA UYAGUARI CHALCO

1.1.2. Código 45785

1.1.3. **Director sugerido:** Ing. Esteban Crespo M.

1.1.4. **1.1.3 Codirector (opcional):** _____

1.1 Tribunal: Ings. Juan Córdova y Rubén Ortega

1.2 Título propuesto: AUDITORIA DE LA GESTION DE SEGURIDAD INFORMATICA DE LA UNIDAD EDUCATIVA PARTICULAR LA ASUNCION BASADA EN COBIT 5

1.3 Resolución:

1.3.1 Aceptado sin modificaciones _____

1.3.2 Aceptado con las siguientes modificaciones:

- INCLUIR EN RIESGOS Y SUPUESTOS, EL RIESGO DE QUE NO EXISTAN PROCESOS. EN CUYO CASO DEBE CONSIDERARSE EL LEVANTAR Y DISEÑAR PROCESOS BASADOS EN COBIT.
- ESPECIFICAR LOS ENTREGABLES EN LOS OBJETIVOS ESPECIFICOS.

1.1.1 Responsable de dar seguimiento a las modificaciones (designado por la Junta Académica de entre los Miembros del Tribunal): Ing. Esteban Crespo M.

1.1.2 No aceptado

- Justificación:

_____

_____

_____

Tribunal

.....	.....
Ing. Esteban Crespo M.	Ing. Juan Córdova O.
.....	.....
Ing. Rubén Ortega L.	Srtal Jessica Uyaguari Ch.
.....	.....
Secretario de Facultad	

Fecha de sustentación: 6 - NOVIEMBRE/2014

RÚBRICA PARA LA EVALUACIÓN DEL PROTOCOLO DE TRABAJO DE TITULACIÓN

1.1.1. **1.1Nombre del estudiante:** JESSICA PAOLA UYAGUARI CHALCO
1.1.2. Código 45785
1.1.3. **Director sugerido**: Ing. Esteban Crespo M.
1.1.4. 1.3 **Codirector (opcional)**:
1.1 1.4. **Título propuesto:** AUDITORIA DE LA GESTION DE SEGURIDAD INFORMATICA DE LA UNIDAD EDUCATIVA PARTICULAR LA ASUNCION BASADA EN COBIT 5
1.2 Revisores (tribunal): Ings. Juan Córdova y Rubén Ortega
1.3 Recomendaciones generales de la revisión:

	Cumple totalmente	Cumple parcialmente	No cumple	Observaciones (*)
Línea de investigación				
1. ¿El contenido se enmarca en la línea de investigación seleccionada?	✓			
Título Propuesto				
2. ¿Es informativo?	✓			
3. ¿Es conciso?	✓			
Estado del arte				
4. ¿Identifica claramente el contexto histórico, científico, global y regional del tema del trabajo?	✓			
5. ¿Describe la teoría en la que se enmarca el trabajo	✓			
6. ¿Describe los trabajos relacionados más relevantes?	✓			
7. ¿Utiliza citas bibliográficas?	✓			
Problemática y/o pregunta de investigación				
8. ¿Presenta una descripción precisa y clara?	✓			
9. ¿Tiene relevancia profesional y social?	✓			
Hipótesis (opcional)				
10. ¿Se expresa de forma clara?	✓			
11. ¿Es factible de verificación?	✓			
Objetivo general				
12. ¿Concuerda con el problema formulado?	✓			
13. ¿Se encuentra redactado en tiempo verbal infinitivo?	✓			
Objetivos específicos				
14. ¿Concuerdan con el objetivo general?	✓			
15. ¿Son comprobables cualitativa o cuantitativamente?	✓			
Metodología				
16. ¿Se encuentran disponibles	✓			

los datos y materiales mencionados?				
17. ¿Las actividades se presentan siguiendo una secuencia lógica?	/			
18. ¿Las actividades permitirán la consecución de los objetivos específicos planteados?	/			
19. ¿Los datos, materiales y actividades mencionadas son adecuados para resolver el problema formulado?	/			
Resultados esperados				
20. ¿Son relevantes para resolver o contribuir con el problema formulado?	/			
21. ¿Concuerdan con los objetivos específicos?	/			
22. ¿Se detalla la forma de presentación de los resultados?	/			
23. ¿Los resultados esperados son consecuencia, en todos los casos, de las actividades mencionadas?	/			
Supuestos y riesgos				
24. ¿Se mencionan los supuestos y riesgos más relevantes?		/		
25. ¿Es conveniente llevar a cabo el trabajo dado los supuestos y riesgos mencionados?	/			
Presupuesto				
26. ¿El presupuesto es razonable?	/			
27. ¿Se consideran los rubros más relevantes?	/			
Cronograma				
28. ¿Los plazos para las actividades son realistas?	/			
Referencias				
29. ¿Se siguen las recomendaciones de normas internacionales para citar?	/			
Expresión escrita				
30. ¿La redacción es clara y fácilmente comprensible?	/			
31. ¿El texto se encuentra libre de faltas ortográficas?	/			

(*) Breve justificación, explicación o recomendación.

- Opcional cuando cumple totalmente,
- Obligatorio cuando cumple parcialmente y NO cumple.

.....

.....

.....

.....

Ing. Esteban Crespo M.

Ing. Juan Córdova O.

Ing. Rubén Ortega L.

Cuenca, 6 de noviembre del 2014

Señor Ingeniero

Xavier Ortega Vasquez

Decano de la Facultad de Ciencias de la Administración

De mis consideraciones,

Luego de enviarle un cordial saludo, me permito informarle que luego de la sustentación del diseño de tesis de la Srta. Jessica Uyaguari con tema de tesis "Auditoría de la Gestión de Seguridad Informática de la Unidad Educativa Particular "La Asunción", basada en Cobit 5" se procedió con la aprobación del mismo una vez que se realice la siguiente modificación: Al objetivo específico incluir los entregables, se ha pedido suprimir el texto "*a través de 5 dimensiones claves: el liderazgo, la innovación, el emprendimiento social, la pro actividad y la comunicación.*", así como el de alinear el cronograma a los objetivos específicos.

He procedido con la verificación de que se haya superado la observación emitida por los miembros del tribunal, por cuanto certifico, como director de tesis, que el cambio del objetivo general ha sido modificado.

Para los fines pertinentes, suscribo de Usted.

Atentamente,

Ing. Esteban Crespo Martínez, MBA

GUIA PARA LA ELABORACIÓN Y PRESENTACIÓN DE LA DENUNCIA/PROTOCOLO DE TRABAJO DE TITULACIÓN

1. DATOS GENERALES

1.1 Nombre del estudiante: Uyaguari Chalco Jessica Paola

1.1.1 Código: 45785

1.1.2 Contacto:

Teléfonos

Convencional: 2901181

Celular: 0987147149

Correo electrónico: ua045785@uazuay.edu.ec

1.2 Director sugerido: Crespo Martínez Paul Esteban Ing.

1.2.1 Contacto:

Teléfonos

Convencional:

Celular: 0996804562

Correo electrónico: ecrespo@uazuay.edu.ec

1.4 Asesor Metodológico:

Salgado Arteaga Francisco Rodrigo, Ph. D.

1.5 Tribunal designado:

1.6 Aprobación:

Junta Académica:

Consejo de Facultad:

1.7 Línea de Investigación de la carrera:

Código UNESCO

Línea: 1203 Informática de Computadores

Programa: 1203.99 Sistemas de Seguridad de la Información

1.7.1 Tipo de trabajo:

El presente es un trabajo informativo e investigativo porque a través de la auditoria de la gestión de seguridad en la red de datos se sugerirá decisiones de mejora o cambio en la red de datos de la Unidad Educativa Particular "La Asunción".

1.8 Área de estudio:

El área de estudio que engloba al presente trabajo es la materia de Auditoria y Seguridad de Sistemas

1.8 Título propuesto:

"Auditoria de la Gestión de Seguridad Informática de la Unidad Educativa Particular "La Asunción" basada en COBIT 5"

1.9 Estado del proyecto:

Este es un proyecto aplicado, basado en el estudio y dominio de COBIT, con la que se pretende realizar la auditoria informática de la Unidad Educativa Particular "La Asunción" a fin de detectar vulnerabilidades y sugerir alternativas para la mitigación de los mismos.

2. CONTENIDO

2.1 Motivación de la investigación:

El motivo de la investigación propuesta surge a partir de que en todo ámbito empresarial, institucional, gubernamental, etc., existe la necesidad de obtener información oportuna y confiable, para la toma de decisiones, con respecto al desarrollo o mejora de la seguridad informática.

Comúnmente la mayoría de las instituciones, no contratan auditores externos para el análisis y diagnóstico de redes de datos, sin considerar que el administrador de red de la institución se convierte en juez y parte a la vez; y esto impide la detección de fallos y debilidades íntegras de la red.

Por consiguiente, la motivación de esta investigación es participar activamente como auditor externo de la red de datos de la institución, con el fin de detectar debilidades y señalar fallas que ayuden a la mejora misma.

2.2 Problemática:

La Unidad Educativa Particular "La Asunción" tiene muchos años de vida institucional y durante este lapso ha tenido significativos cambios y crecimiento en todas sus áreas, incluyendo el Departamento de Cómputo.

En cuanto a los sistemas y redes que rigen la misma no ha recibido auditoría externa en gestión de seguridad Informática, sin embargo se audita de forma interna.

Dicha auditoria ha permitido realizar ciertos cambios y mejoras, pero no está de acuerdo a su crecimiento y necesidades. Además, con las auditorías internas puede surgir un gran problema como el mencionado anteriormente, que el administrador de red sea juez y parte de la institución a cargo; evitando así que se detecten falencias, debilidades o mejoras que se pudieron realizar en la red de esta institución.

Este problema se ve reflejado claramente en la Unidad Educativa Particular "La Asunción"; razón por la cual este trabajo de investigación, tiene como objetivo realizar auditoria en la red de datos de la institución, con la cual se podrá mejora significativamente a la misma.

2.3 Pregunta de investigación:

¿Qué impacto tendrá la presente auditoria en la seguridad de la red de datos de la Unidad Educativa La Asunción?

2.4 Resumen:

Hoy en día muchas entidades públicas o privadas no cuentan con el asesoramiento adecuando sobre la seguridad en su red de datos; y se ven reflejadas en malas decisiones; otras empresas son auditadas internamente con la finalidad de reducir gastos, y no consideran las desventajas de este tipo de auditorías.

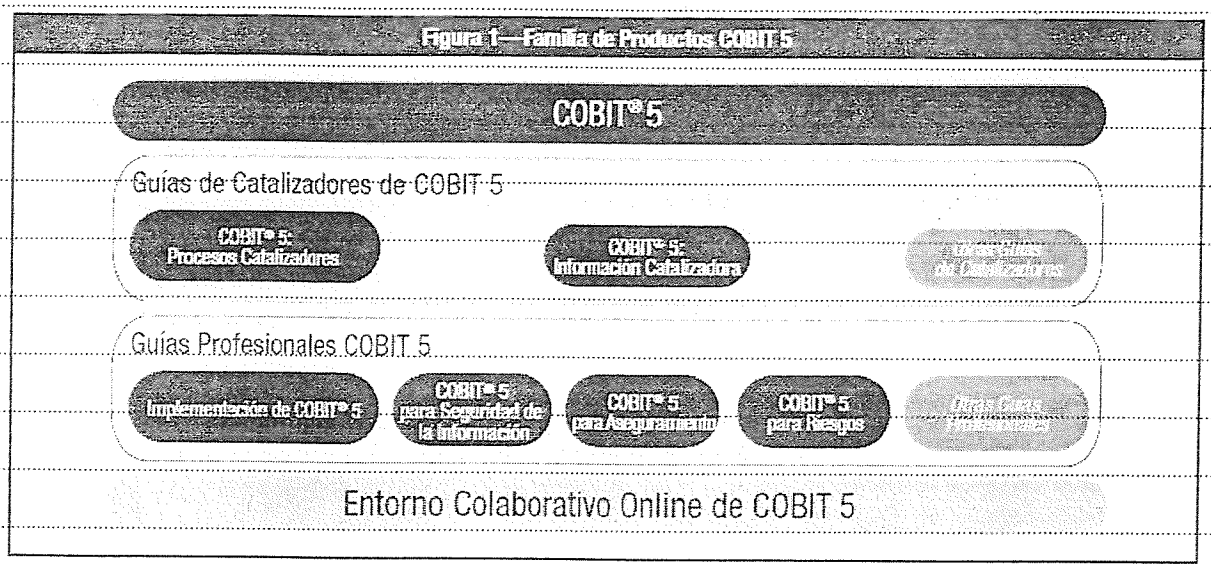
Este es el caso de la Unidad Educativa Particular la Asunción, la cual no cuenta con una adecuada auditoria sobre su seguridad en la red de datos. Es por ello que la tesis propuesta hace énfasis en la realización de una auditoria externa, que involucra grandes beneficios para la misma, en cuanto a la identificación y eliminación de debilidades y riesgos, mejorar las seguridades existentes y realizar nuevas propuestas de unidad.

Para la realización de la auditoría propuesta, ésta estará fundamentada en COBIT (Control Objectives for Information and related Tecnology), ya que cumple con las normas, técnicas y estándares que rigen los procesos de auditoria actual y se rige a la legislación informática vigente en el Ecuador.

Se puede decir que COBIT es el mejor marco de referencia para la ejecución de auditorías por ser un estándar que asocia las mejores prácticas para el control de TI; estas características lo han posicionado como uno de los modelos más utilizados en el mundo por usuarios, directivos y auditores.

Vale recalcar que se adjunta la respectiva aprobación por parte de la Unidad Educativa para la realización de la Auditoría en sus instalaciones.

2.5 Indagación Exploratoria y Base Conceptual



COBIT 5: Un marco de negocio para el gobierno y la gestión de las TI de la empresa

"El marco COBIT 5 se construye sobre cinco principios básicos, que quedan cubiertos en detalle e incluyen una guía exhaustiva sobre los catalizadores para el gobierno y la gestión de las TI de la empresa.

La familia de productos de COBIT 5 incluye los siguientes productos:

• COBIT 5 (el marco de trabajo)

• Guías de catalizadores de COBIT 5, en las que se discuten en detalle los catalizadores para el gobierno y gestión, estas incluyen:

– COBIT 5: Información Catalizadora

– Información posibilitadora (en desarrollo)

– Otras guías de catalizadores (visitar www.isaca.org/cobit)

• Guías profesionales de COBIT 5, incluyendo:

– Implementación de COBIT 5

(ISACA, 2012)

– COBIT 5 para Seguridad de la Información (en desarrollo)

– COBIT 5 para Aseguramiento (en desarrollo)

– COBIT 5 para Riesgos (en desarrollo)

– Otras guías profesionales (visitar www.isaca.org/cobit)

• Un entorno colaborativo online, que estará disponible para dar soporte al uso de COBIT 5" (ISACA, 2012)

Según se muestra en la Figura1- Familia de Productos COBIT 5

(ISACA, 2012)

Beneficios de COBIT hoy en día según (ISACA, 2012) (www.isaca.org/cobit):

- Compendio de mejores prácticas aceptadas internacionalmente
- Orientado al gerenciamiento de las tecnologías
- Complementado con herramientas y capacitación
- Gratuito
- Respaldado por una comunidad de expertos

- En evolución permanente
- Mantenido por una organización sin fines de lucro, con reconocimiento internacional
- Relacionado con otros estándares
- Orientado a Procesos, sobre la base de Dominios de Responsabilidad

Sistemas Informáticos

Como se describe en el artículo de (Informática Hoy, s.f.) Podemos decir que un sistema Informático resulta de la interacción entre los componentes físicos que se denominan Hardware y los lógicos que se denominan Software. A estos hay que agregarles el recurso humano, parte fundamental de un sistema informático. Este componente es llamado Humanware.

Un sistema Informático recibe información a través de periféricos de entrada, la cual es procesada por periféricos de salida.

Es importante no confundir dos términos, en esta tesis propuesta hablamos de Sistemas Informáticos no de sistemas de información; al referirnos a sistemas informáticos hacemos referencia al Hardware + comunicación + Software.

2.6 Objetivo general:

Auditar la seguridad en la red de datos de la Unidad Educativa Particular "La Asunción".

2.7 Objetivos específicos:

- Fundamentar teóricamente la auditoria de seguridad de redes de datos
- Elaborar un plan de auditoria
- Ejecutar la auditoría y emitir un informe detallado de los resultados de la misma, incluyendo las observaciones y sus respectivas recomendaciones, basados en COBIT

2.8 Metodología:

La metodología a utilizarse en la realización de la tesis será, la metodología exploratoria ya que se pretende auditar la red de datos de la unidad educativa "La Asunción" con la finalidad de detectar debilidades, fortalezas y riesgos de la misma.

La utilización de esta metodología es con el objetivo de ver resultados obtenidos de la auditoría realizada por personal que no pertenece a la institución.

2.9 Alcances y resultados esperados:

Como resultado a los objetivos específicos propuestos anteriormente se obtendrá un informe de auditoría basado en COBIT 5 para seguridad de la información dentro del dominio principal de gestión y en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y

supervisar; se realizara la auditoria con el dominio de Supervisar, Evaluar y Valorar (Monitor, Evaluate and Assess; MEA)

2.10 Supuestos y riesgos:

Riesgos Técnicos

- Los equipos a auditarse son susceptibles a daños y por ende se podría perder la información guardada en la red de datos.

Alternativas de Solución

- Obtener un respaldo sobre la seguridad en la red de datos y de los equipos.
- Investigar y proponer con anticipación herramientas compatibles con el sistema operativo.

Riesgos Externos

- Por parte de la Unidad educativa haya cierto recelo de la información y no se pueda realizar la auditoria correctamente.
- No existan procesos que puedan ser auditables.

Alternativas de Solución

- Evaluar adecuadamente las herramientas a utilizar antes de empezar el desarrollo de la tesis.
- Obtener la debida aprobación por parte de la Unidad Educativa; para realizar la auditoría sin ningún inconveniente.
- Leer detenidamente los requisitos para la presentación del diseño de tesis y elaborar correctamente el mismo, evitando así que se postergue la aprobación de la misma.
- En caso de no existir los procesos, se deben crear, diseñar, auditar y calcular el nivel de madurez del mismo

2.11 Presupuesto:

Rubro-Denominación	Costo USD (detalle)	Justificación ¿para qué?
Papel A4	$30	Papel para imprimir la tesis
Internet	$180	Investigación sobre la herramienta Oracle.
Empastados	$30	Presentación Final de la Tesis
Impresión	$50	Impresión documento de la Tesis
Hojas membretadas de la Universidad	$5	Se requiere para la denuncia de la tesis.
Transporte	$40	Movilización a la Universidad para ajustes correspondientes a la tesis.
		Movilización a la Unidad Educativa para la realización de la Auditoría.
Gastos Varios	$25	Gastos inesperados arreglo de computador portátil, alimentación.

Adquisición de COBIT 5	0	0
TOTAL	360	

2.12 Financiamiento:

El proyecto será autofinanciado, esperando que los resultados sean lo mejores.

2.13 Esquema tentativo:

Resumen

Abstract

Introducción

Objetivos

CAPITULO I Fundamentos generales

Introducción
Historia
Misión
Alcance
Gestión de Seguridad
Estructura del estándar COBIT

CAPITULO II Situación actual de la Unidad Educativa "La Asunción"

Descripción
Estructura orgánico-funcional General
Estructura orgánico-funcional del departamento de Sistemas
Infraestructura

CAPITULO III Plan de Auditoría para la gestión de Red

Alcance
Comunicado al Rectorado sobre el inicio de actividades
Procesos COBIT aplicables a la gestión de seguridad
Herramientas útiles para el desarrollo de la auditoría
Plan de Auditoría

CAPITULO IV Ejecución del plan Auditoría.

Procesos en el dominio de supervisar, evaluar y valorar
Proceso de Cronograma de la Auditoría

CAPITULO V Informes de auditoría (Técnico y Gerencial)

Análisis de los resultados Obtenidos
Informe final de la auditoría realizada
Ejecución de algunos procesos

CAPITULO VI Conclusión Y Recomendaciones

Conclusiones

Recomendaciones

Referencia Bibliográfica

Glosario

Anexos

2.14 Cronograma:

Objetivo Específico	Actividad	Resultado Esperado	Tiempo(Seman
Fundamentar teóricamente la auditoria de seguridad de redes de datos	Fundamentos generales	Introducción Historia Misión Alcance Gestión de Seguridad Estructura del estándar COBIT	5 Semanas
	Situación actual de la Unidad Educativa "La Asunción"	Descripción Estructura orgánico-funcional General Estructura orgánico-funcional del departamento de Sistemas Infraestructura	
- Elaborar un plan de auditoria	Plan de Auditoría para la gestión de Red	Alcance Comunicado al Rectorado sobre el inicio de actividades Procesos COBIT aplicables a la gestión de seguridad Herramientas útiles para el desarrollo de la auditoría Plan de Auditoría	6 Semanas

- Ejecutar la auditoría y emitir un informe detallado de los resultados de la misma, incluyendo las observaciones y sus respectivas recomendaciones, basados en COBIT	Ejecución del plan Auditoría.	Procesos en el dominio de supervisar, evaluar y valorar Proceso de Cronograma de la Auditoría	8 Semanas
	Informes de auditoría (Técnico y Gerencial)	Análisis de los resultados Obtenidos Informe final de la auditoría realizada	
	Conclusión Y Recomendaciones	Ejecución de algunos procesos Conclusiones Recomendaciones Documentación para la Tesis.	

2.15 Referencias:

COBIT 5 EN ESPAÑOL. « Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.» Personal Copy of: PABLO CONDE MERCADO.

www.isaca.org/cobit

(Informática Hoy, s.f.)

2.15 Firma de responsabilidad (estudiante)

2.16 Firma de responsabilidad (director sugerido)

2.18 Fecha de Entrega: 11/12/2014

UNIVERSIDAD DEL AZUAY

DOCTORA JENNY RIOS COELLO SECRETARIA, DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN DE LA UNIVERSIDAD DEL AZUAY

C E R T I F I C A:

Que, la Señorita Jessica Paola Uyaguari Chaleo, registrada con código 45785 perteneciente a la Escuela Sistemas y Telemática, luego de cumplir con todas las asignaturas de su Pensum de estudios, egresó de la Facultad el día 26 de Julio de 2014.

Cuenca, Octubre 31 del 2014

Derecho 111022
vcf.-

0651794

Oficio Nro. 126-2014-DIST-UDA

Cuenca, 28 de Octubre de 2014

Señor Ingeniero
Xavier Ortega Vázquez
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMNISTRACIÓN
Presente.-

De nuestras consideraciones:

La Junta Académica de la Escuela de Ingeniería de Sistemas y Telemática, reunida el día 28 de Octubre del 2014, recibió el proyecto de tesis titulado "Auditoría de la gestión de seguridad informática de la Unidad Educativa Particular La Asunción basada en COBIT 5", presentada por la estudiante Jessica Uyaguari Chalco, estudiante de la Escuela de Ingeniería de Sistemas y Sistemas y revisado por el Ing. Esteban Crespo previo a la obtención del título de Ingeniero de Sistemas y Telemática.

La Junta solicita por su digno intermedio notificar al tribunal designado y determinar lugar, fecha y hora de sustentación.

Por lo expuesto, y de conformidad con el Reglamento de Graduación de la Facultad, recomienda como director y responsable de aplicar cualquier modificación al diseño del trabajo de graduación posterior a al Ing. Esteban Crespo y como miembros del Tribunal al Ing. Juan Córdova y Ing. Rubén Ortega.

Atentamente,

Ing. Marcos Orellana Cordero
Director Escuela de Ingeniería de Sistemas y Telemática
Universidad del Azuay

Cuenca, 28 de octubre de 2014

Ing.

Xavier Ortega Vásquez, MBA

Decano de la Facultad de Ciencias de la Administración

Presente

De mi consideración:

Por la presente, me permito informarle que he revisado el diseño de tesis presentado por la estudiante **Jessica Paola Uyaguari Chalco** con el tema *"Auditoria de la Gestión de Seguridad Informática de la Unidad Educativa Particular "La Asunción" basada en Cobit 5"*, como requisito previo para la obtención del título de Ingeniero de Sistemas y Telemática.

Al respecto, el diseño de tesis presenta una estructura teórica, metodológica y técnica coherente, cuyo objetivo es realizar la auditoria informática de la unidad educativa "La Asunción", a manera de poder detectar el cumplimiento de los procesos relacionados con Informática, aplicando el modelo COBIT versión 5.

Por lo expuesto, emito informe favorable y recomiendo su aprobación.

Ing. Esteban Crespo Martínez, MBA

UNIVERSIDAD DEL AZUAY

Cuenca, Octubre 29 del 2014

Ing.
Xavier Ortega Vázquez
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
Ciudad.

De mis consideraciones:

Yo, Jessica Paola Uyaguari Chalco, con código universitario No. 045785, me dirijo a usted con el objeto de solicitarle se digne disponer a quien corresponda, para que se proceda con la revisión de la denuncia del trabajo de titulación, con el siguiente tema: Auditoria de Gestión de la Seguridad Informática de la Unidad Educativa Particular "La Asunción", basada en COBIT.

Por la acogida que sabrá dispensar a la presente, le anticipo mis sinceros agradecimientos.

De usted muy atentamente,

JESSICA UYAGUARI CHALCO
C.I. 0104985296

Recibí el original N° 0651795