AUDITORIA DE SISTEMAS APLICADA AL SISTEMA DE INFORMACIÓN DE LA COOPERATIVA DEL MAGISTERIO DE TUQUERRES COACREMAT

JOSÉ ALEXANDER MELO IPÚJAN

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2013

AUDITORIA DE SISTEMAS APLICADA AL SISTEMA DE INFORMACIÓN DE LA COOPERATIVA DEL MAGISTERIO DE TUQUERRES COACREMAT

JOSÉ ALEXANDER MELO IPÚJAN

Trabajo de grado presentado como requisito parcial para optar al título de Ingeniero de Sistemas

Director:
ING. MANUEL BOLAÑOS GONZALES

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2013

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones aportadas en este Trabajo de Grado son responsabilidad de los autores.

Artículo 1 del Acuerdo No. 324 de octubre 11 de 1966, emanado del honorable Consejo Directivo de la Universidad de Nariño.

Las ideas y conclusiones aportadas en este trabajo de grado son exclusivas de sus autores, por lo tanto la Universidad de Nariño no tiene ninguna responsabilidad".

Artículo 13º del acuerdo No. 005 de Enero 26 de 2010 emanado del Honorable Consejo Académico de la Universidad de Nariño.

Nota de aceptación

_____
_____
_____
_____
_____

_____
JURADO

_____
JURADO

_____
JURADO

San Juan de Pasto, Diciembre de 2013

AGRADECIMIENTOS

A Dios, Mi Madre y Mi hermano por el apoyo incondicional que recibo por parte de ellos para lograr objetivos y cumplir metas a pesar de todos los problemas que se encuentra en el camino.

A mi familia, por estar presente en todos los momentos

Al ingeniero Manuel Bolaños, por ser mi guía en este proyecto

A mis amigos, compañeros y conocidos

DEDICATORIA

Dedicado a mi madre María Carmen Ipújan por ser la persona que
Siempre me acompaño y estuvo con migo en todo momento
Dándome fuerzas para lograr este triunfo, es a ella
A quien debo toda mi vida y todos mis logros
No podre pagar nunca lo que has hecho por mí. Madre, te amo
Gracias y mil bendiciones para ti.

RESUMEN

El presente trabajo, describe la Auditoría de sistemas realizada a la COOPERATIVA DEL MAGISTERIO DE TUQUERRES – COACREMAT. Utilizando COBIT, una herramienta desarrollada para, ayudar a identificar posibles vulnerabilidades dentro del sistema de información en la seguridad física, seguridad lógica, plataforma tecnológica y redes implementando las buenas prácticas de COBIT que están enfocadas en el ambiente de un control óptimo que debe tener una empresa para lograr una alineación efectiva de las TI y los objetivos de negocio.

Se seleccionaron los dominios y procesos que involucran al sistema de información de Coacremat y se hizo los diferentes análisis para desarrollar la auditoria de sistemas, arrojando varias falencias así como sus posibles soluciones.

De acuerdo a los resultados obtenidos en las encuestas, entrevistas y pruebas cuantitativas todos estos resultados con cada objetivo de control, que propone COBIT, se presentaron las observaciones y recomendaciones emitidas en un informe a la Gerencial.

ABSTRACT

This paper describes the systems audit conducted to COOPERATIVE OF TEACHERS OF TUQUERRES - COACREMAT . Using COBIT, a tool developed to help identify potential vulnerabilities in the information system physical security, logical security , technology platform and networks implementing the best practices of COBIT that are focused on the environment of optimal control must have a company to achieve effective alignment of IT and business objectives .

Domains and processes involving the information system Coacremat and different analysis was done to develop systems audit , throwing several shortcomings and possible solutions were selected.

According to the results of surveys , interviews and quantitative evidence these results with each control objective , proposed COBIT , observations and recommendations contained in a report presented to the Management .

CONTENIDO

Pág.

INTRODUCCION 20
1. TITULO 26
2. MARCO TEORICO 27
2.1 ASPECTOS GENERALES SOBRE LA AUDITORIA 27
2.2 TIPOS DE AUDITORIA 27
2.2.1 Auditoría Interna. 27
2.2.2 Auditoría externa 28
2.2.3 Auditoria de sistemas 28
2.2.4 Auditoria informática. 28
2.4 AUDITORIA DE SISTEMAS COMO OBJETO DE ESTUDIO 29
2.4.1 Alcance de la auditoria de sistemas 29
2.4.2 Objetivos de la auditoria de sistemas: 30
2.4.3 Principales pruebas y herramientas para efectuar una auditoría de sistemas 30
2.4.4 Perfiles Profesionales de los auditores informáticos: 31
2.4.5 Pasos a seguir para una auditoria de sistemas en una organización: 32
2.5 METODOLOGÍAS DE AUDITORIA DE SISTEMAS 35
2.5.1 COBIT (Control objectives for information and related technology: 37
2.6 TÉCNICAS DE AUDITORIA DE SISTEMAS 58
2.6.1 Selección de áreas de auditoria. 58
2.6.2 Sistema de puntajes (Scoring). 58
2.6.3 Técnicas para operacionalizar la función de auditoría: 58
2.6.4 Técnicas para examinar programas aplicativos: 59
3. METODOLOGÍA 60
4. DESARROLLO DEL TRABAJO 62
4.1 ARCHIVO PERMANENTE 62

4.1.1 Cooperativa del magisterio de Túquerres – Coacremat 62
4.1.1.1 Misión 62
4.1.1.2 Visión 62
4.1.1.3 Historia de la cooperativa del magisterio de Tuquerres 62
4.1.1.4 Departamento de sistemas 64
4.1.1.5 Organigrama Coacremat 65
4.2 ARCHIVO CORRIENTE 67
4.2.1 Plan de auditoria 67
4.2.1.1 Objetivos: 67
4.2.1.4 Alcance 67
4.2.1.5 Justificación 68
4.2.1.6 Metodología 68
4.2.1.7 Herramientas de estudio: 69
4.2.1.8 Recursos 70
4.2.2. Programa de auditoria 70
4.2.1.1 Objetvos de control para la cooperativa del magisterio de Tuquerres: 70
4.2.3 Hallazgos. 92
4.2.3.1 Procesos Auditados en cooperativa del magisterio de Túquerres – Coacremat: 92
4.2.3.2 Hallazgos planificación y organización (PO): 93
4.2.3.2 Resultado Matriz de probabilidad dominio Adquirir e implementar (AL) 102
4.2.3.3 Hallazgos dominio: adquirir e implementar (AL). 103
4.2.3.4 Resultado matriz de probabilidad dominio entregar y dar soporte (DS) 110
4.2.3.5 Hallazgos entregar y dar soporte (DS). 110
4.2.3.6 Resultado matriz de probabilidad dominio monitorear y evaluar (ME) 127
4.2.3.7 Hallazgos monitorear y evaluar (ME). 127
5. INFORME DE AUDITORIA 130
6. INFORME GERENCIAL 144
7. CONCLUSIONES 147

8. RECOMENDACIONES 148
REFERENCIAS BIBLIOGRAFICAS..... **¡Error! Marcador no definido.**
ANEXOS 150

LISTADO DE TABLAS

Pág.

Tabla 1: Perfiles profesionales y actividades 31

Tabla 2: Definición de fuentes de conocimiento, pruebas de análisis de auditoria 84

Tabla 3: Cuestionario cuantitativo 87

Tabla 4: Matriz de probabilidad de ocurrencia e impacto según relevancia del proceso 89

Tabla 5: Hallazgos 91

Tabla 6: Hallazgo 1 ACMT 94

Tabla 7: Hallazgo 2 ACMT 96

Tabla 8: Hallazgo 3 ACMT 98

Tabla 9: Hallazgo 4 ACMT 100

Tabla 10: Hallazgo 1 ACMT 103

Tabla 11: Hallazgo 2 ACMT 105

Tabla 12: Hallazgo 3 ACMT 107

Tabla 13: Hallazgo 4 ACMT 108

Tabla 14: Hallazgo 1 ACMT 111

Tabla 15: Hallazgo 2 ACMT 113

Tabla 16: Hallazgo 3 ACMT 115

Tabla 17: Hallazgo 4 ACMT 117

Tabla 18: Hallazgo 5 ACMT 119

Tabla 19: Hallazgo 6 ACMT 121

Tabla 20: Hallazgo 7 ACMT 122

Tabla 21: Hallazgo 8 ACMT 124

Tabla 22: Hallazgo 1 ACMT 128

LISTADO DE FIGURAS

Pág.

Figura 1: Las tres dimensiones conceptuales de COBIT 57

GLOSARIO

Activo: En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tiene valor para la organización.

Alerta: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Amenaza: Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Según [ISO/IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Aplicación: Aunque se suele utilizar indistintamente como sinónimo genérico de 'programa' es necesario subrayar que se trata de un tipo de programa específicamente dedicado al proceso de una función concreta dentro de la empresa.

Archivo de datos: Cualquier archivo creado dentro de una aplicación: por ejemplo, un documento creado por un procesador de textos, una hoja de cálculo, una base de datos o un gráfico. También denominado Documento.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Bases de Datos: Colección de datos organizada de tal modo que el ordenador pueda acceder rápidamente a ella. Una base de datos relacionar es aquella en la que las conexiones entre los distintos elementos que forman la base de datos están almacenadas explícitamente con el fin de ayudar a la manipulación y el acceso a éstos.

Checklist: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

Cliente: Cliente o 'programa cliente' es aquel programa que permite conectarse a un determinado sistema, servicio o red.

COBIT (Objetivos de Control de las Tecnologías de la Información y Tecnologías Relacionadas) Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacionales y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados. Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida.

Conexión física: Permiten a las computadoras transmitir y recibir señales directamente. Las conexiones físicas están definidas por el medio empleado (pueden ser cables hasta satélites) para transmitir la señal, por la disposición geométrica de las computadoras (topología) y por el método usado para compartir información, desde textos, imágenes y hasta videos y sonidos.

Criptografía: Ciencia dedicada al estudio de técnicas capaces de conferir seguridad a los datos. El cifrado es fundamental a la hora de enviar datos a través de las redes de telecomunicaciones con el fin de conservar su privacidad.

Datos: Término general para la información procesada por un ordenador.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento: Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.

Factibilidad: Es la disponibilidad de los recursos necesarios para llevar a cabo los objetivos o metas señaladas, sirve para recopilar datos relevantes sobre el desarrollo de un proyecto y en base a ello tomar la mejor decisión.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Hardware: Conjunto de dispositivos de los que consiste un sistema. Comprende componentes tales como el teclado, el Mouse, las unidades de disco y el monitor.

Impacto: El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros ej., pérdida de reputación, implicaciones legales, etc.

Incidente: Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Internet: Interconexión de redes informáticas que permite a las computadoras conectadas comunicarse directamente.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISACA: Information Systems Audit and Control Association. Publica COBIT y emite diversas acreditaciones en el ámbito de la seguridad de la información.

LAN (Local Área Network – Red de Área Local): Interconexión de computadoras y periféricos para formar una red dentro de una empresa u hogar, limitada generalmente a un edificio.

Metodología: Conjunto de métodos utilizados en la investigación científica

Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

Objetivo: Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad de TI determinada.

Papeles de trabajo: Registra el planeamiento, naturaleza, oportunidad y alcance de los procedimientos de auditoría aplicados por el auditor y los resultados y conclusiones extraídas a la evidencia obtenida. Se utilizan para controlar el progreso del trabajo realizado para respaldar la opinión del auditor. Los papeles de trabajo pueden estar constituidos por datos conservados en papel, película, medios electrónicos u otros medios.

Password: Conocida también como 'clave de acceso'. Palabra o clave privada utilizada para confirmar una identidad en un sistema remoto que se utiliza para que una persona no pueda usurpar la identidad de otra.

Plan de contingencia: Es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudara a controlar una situación de emergencia y minimizar sus consecuencias negativas.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:2005]: intención y dirección general expresada formalmente por la Dirección.

Procedimiento: Método o sistema estructurado para la ejecución de actividades.
En computación, una subrutina o subprograma, como idea general, se presenta como un algoritmo separado del algoritmo principal, el cual permite resolver una tarea específica.

Proceso: Conjunto de operaciones lógicas y aritméticas ordenadas, cuyo fin es la obtención de resultados.

Programa: Secuencia de instrucciones que obliga al ordenador a realizar una tarea determinada.

Programa cliente: Programa cliente o simplemente 'cliente' es aquel programa que permite conectarse a un determinado sistema, servicio o red.

Red: Servicio de comunicación de datos entre ordenadores. Conocido también por su denominación inglesa: 'network'. Se dice que una red está débilmente conectada cuando la red no mantiene conexiones permanentes entre los ordenadores que la forman. Esta estructura es propia de redes no profesionales con el fin de abaratar su mantenimiento.

Repositorio: Donde se almacenan los elementos definidos o creados por la herramienta, y cuya gestión se realiza mediante el apoyo de un Sistema de Gestión de Base de Datos (SGBD) o de un sistema de gestión de ficheros

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Router: Es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un router (mediante bridges), y que por tanto tienen prefijos de red distintos.

Segregación de tareas: Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

Servidor: Ordenador que ejecuta uno o más programas simultáneamente con el fin de distribuir información a los ordenadores que se conecten con él para dicho fin. Vocablo más conocido bajo su denominación inglesa 'server'.

Sistema de información: Se denomina Sistema de Información al conjunto de procedimientos manuales y/o automatizados que están orientados a proporcionar información para la toma de decisiones.

Software: Componentes inmateriales del ordenador: programas, sistemas operativos, etc.

Switch: Dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar

dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

TI: Tecnologías de Información

Técnica: La técnica es el procedimiento o el conjunto de procedimientos que tienen como objetivo obtener un resultado determinado, ya sea en el campo de la ciencia, de la tecnología, de las artesanías o en otra actividad

Tratamiento de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

Valoración de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

INTRODUCCION

La auditoría de sistemas se ha constituido en una de las herramientas más poderosas para realizar control a cualquier organización empresarial en los sistemas de información de la organización donde se requiere el desarrollo, la generación y la promulgación de normas para lograr una gestión integral de las Tic.

Es importante conocer los estándares que Cobit como una de las principales técnicas de auditoría presenta al auditor para así realizar la revisión y evaluación de cada uno de los componentes de un sistema y como sus posibles soluciones.
Es por eso que se debe seguir una serie de pasos previos que permitan dimensionar las características y objetivos que se desean estudiar, es por eso que la seguridad informática hace parte importante en una auditoria de sistemas ya que la información y los datos hoy en día son un activo imprescindible dentro de las empresas, donde la información obtenidas de los procesos internos de las organizaciones deben ser protegidas de anomalías y posibles problemas, encontrando en la auditoria una solución a futuro ya que detecta vulnerabilidades antes que sucedan y produzcan un daño irreparable.

Este proyecto de investigación propone auditar al sistema de información de Coacremat de una forma integral donde se evalúa y analiza los componentes que hacen parte de los procesos de datos que arroja la empresa a sus asociados. Identificando sus vulnerabilidades para lograr un mayor confianza de los asociados.

IDENTIFICACIÓN DEL PROBLEMA

Título del proyecto

AUDITORIA DE SISTEMAS APLICADA AL SISTEMA DE INFORMACIÓN DE LA COOPERATIVA DEL MAGISTERIO DE TUQUERRES COACREMAT.

Línea de investigación: Según las líneas de investigación aprobadas y definidas en el Programa de Ingeniería de Sistemas de la Universidad de Nariño, como acuerdo de facultad 045 de octubre 10 de 2002 dado por el consejo de facultad, el proyecto corresponde a la línea de investigación de Sistemas Computacionales, ya que esta línea tiene como objetivo planificar, diseñar, implantar, administrar y evaluar sistemas computacionales y servicios basados en estos sistemas complejos de información, la cual soporta la temática de Auditoria de Sistemas.

DESCRIPCION DEL PROBLEMA

Planteamiento del problema

La cooperativa del magisterio de Túquerres (Coacremat) cuenta con un sistema de información importante el cual no ha sido sometido a ningún tipo de proceso o estudio formal por parte de un ente externo para identificar las posibles vulnerabilidades que se puedan presentar tanto lógicas, físicas, infraestructura tecnológica y software.

El sistema de información contiene errores como el ingreso de nuevos usuarios, eliminación de los mismos, los administradores del sistema no tienen total control de este ya que la empresa contratada por Coacremat no lo deja hacer y tienen que recurrir al soporte cada vez que existe un inconveniente haciendo lentos los procesos.

La red de datos es obsoleta en cuanto al sistema de información, se encuentra desorganizada y en unas partes totalmente desprotegida haciendo vulnerable la información que pasa a través de esta.

Existen zonas como el cuarto donde se encuentra el servidor de la empresa el cual no está adecuado para este tipo de servicio es aquí donde concluyen gran cantidad de terminales de las diferentes zonas del edificio y fuera del, además no se cuenta con un servidor espejo en otro lugar para dar soporte a los datos que se encuentran en la sede principal.

Todas estas conflagraciones hacen que los procesos en el sistema se vuelvan lentos y no seguros ya que la información es abundante y se tiene que decir al asociado de la empresa cuando hace una consulta que espere un tiempo mientras los datos se consultan y se corrigen errores.

Es de vital importancia para la cooperativa del magisterio de Túquerres (Coacremat) corregir los errores ya que el sistema de información seguirá lento y los asociados tendrán dificultades al hacer sus diferentes consultas.

Formulación del Problema: ¿Cómo determinar el nivel de confiabilidad en cuanto a la seguridad física, lógica, infraestructura tecnología y software que permitan realizar recomendaciones que garanticen el buen uso de los recursos y de la información que se maneja en la Cooperativa del Magisterio de Túquerres - Coacremat?

Sistematización del problema:

- ¿Cómo determinar el nivel de confiabilidad de la seguridad física que soportan los procesos del sistema de información que permita establecer las recomendaciones necesarias para garantizar su seguridad?
- ¿Cómo determinar el nivel de confiabilidad de la seguridad lógica que soportan los procesos del sistema de información que permita establecer las recomendaciones necesarias para garantizar su seguridad?
- ¿Cómo determinar el nivel de confiabilidad de la infraestructura tecnológica que soportan los procesos del sistema de información que permita establecer las recomendaciones necesarias para garantizar su buen desempeño?
- ¿Cómo determinar el nivel de confiabilidad del software que soportan los procesos del sistema de información que permita establecer las recomendaciones necesarias para garantizar su seguridad?

OBJETIVOS

Objetivo general

Realizar una auditoría de sistemas para evaluar la seguridad física, seguridad lógica, infraestructura tecnológica y software del sistema de información de Coacremat

Objetivos específicos

- Realizar una auditoría de sistemas para evaluar la confiabilidad de la seguridad lógica en el sistema de información de Coacremat
- Realizar una auditoría de sistemas para evaluar la confiabilidad de la seguridad física en el sistema de información de Coacremat
- Realizar una auditoría de sistemas para evaluar la confiabilidad de la infraestructura tecnológica que se utiliza en el sistema de información de Coacremat
- Realizar una auditoría de sistemas para evaluar la confiabilidad del softwareque se utiliza en el sistema de información de Coacremat

JUSTIFICACIÓN

"*La auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de los elementos de una organización que participan en el procesamiento de la información, a fin de que por medio del*

señalamiento de cursos alterativos se logre una utilización más eficiente de la información que servirá para una eventual toma de decisiones."[1]

La auditoría de sistemas es de gran importancia ya que se encarga de llevar a cabo la evaluación de normas, controles, técnicas y procedimientos para el excelente desempeño de los sistemas de información ya que proporciona controles necesarios para que los sistemas sean confiables y con excelente nivel de seguridad.

Por lo anterior el proceso de auditoría de sistemas se convierte en elemento fundamental y de vital importancia, para determinar los hallazgos y vulnerabilidades más relevantes de seguridad física y lógica que actualmente se presentan el sistema integral de información en la COOPERATIVA DEL MAGISTERIO DE TUQUERRES COACREMAT.

Con la ejecución de la auditoria se beneficia los usuarios de la empresa que se encuentran en sus diferentes sedes en todo el departamento de Nariño, ya que con base a los resultados se podrá tomar las medidas necesarias que permitan optimizar cada una de las tareas relacionadas con el procesamiento de la información.

ALCANCE Y DELIMITACION

En la auditoría de sistemas que se realizó a la cooperativa del magisterio de Túquerres (COACREMAT) permitió ejecutar una evaluación detallada en los siguientes ítems:

Seguridad lógica

Se analizó las diferentes barreras y procedimientos que resguardan el acceso a la información donde se evaluó y determino los riesgos para la integridad de los datos donde los objetivos evaluados fueron:

- Restricción al acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.

[1] ECHENIQE GARCIA José A., Auditoría en informática, segunda edición 2a Ed., Mc Graw Hill D. F. 2005.

- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Seguridad física

Se realizó un análisis a la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.

Se evaluó permanentemente la seguridad física de las instalaciones de cómputo y del edificio donde los ítems a evaluados fueron:

- Desastres naturales, incendios accidentales, tormentas e inundaciones.
- Amenazas ocasionadas por el hombre.
- Disturbios, sabotajes internos y externos deliberados.

Infraestructura tecnológica

Redes de datos

En un sistema de información las redes juegan un papel muy importante ya que estás llevan los datos y la información de la empresa, es a donde se debe determinar la confiabilidad en los siguientes puntos:

- Áreas de equipo de comunicación con control de acceso.
- Protección y tendido adecuado de cables y líneas de comunicación para evitar accesos físicos.
- Control de utilización de equipos de prueba de comunicaciones para monitorizar la red y el tráfico en ella.
- Contraseñas de acceso a la red.
- Garantizar que en una transmisión, ésta solo sea recibida por el destinatario. Para esto, regularmente se cambia la ruta de acceso de la información a la red.
- Registrar las actividades de los usuarios en la red.
- Comunicación web

Equipos de sistemas

Se evaluaron los equipos informáticos con los que cuenta Coacremat ya que es un factor determinante en un sistema informático determinando el grado de confiabilidad.

Software

Se evaluó el software ya que es un activo muy importante al cual se le hizo su respectiva evaluación para determinar las posibles vulnerabilidades informáticas en la cual puede incurrir la empresa donde se determina cómo se adquiere, distribuye y usa el software en la organización.

1. TITULO

"AUDITORIA DE SISTEMAS APLICADA AL SISTEMA DE INFORMACIÓN DE LA COOPERATIVA DEL MAGISTERIO DE TUQUERRES COACREMAT"

2. MARCO TEORICO

2.1 ASPECTOS GENERALES SOBRE LA AUDITORIA

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

La auditoría de sistemas deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

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

2.2 TIPOS DE AUDITORIA

2.2.1 Auditoría Interna. Es una actividad independiente que realiza la empresa y que está encaminada a la revisión de operaciones contables además de la evaluación y medición de la eficacia de otros controles, con la finalidad de prestar un servicio a la dirección. Se aplica mejor en empresas medianas que tienden a aumentar en volumen, extensión geográfica y complejidad y se hace imposible el control directo de las operaciones por parte del director.

El objetivo principal es ayudar a la dirección en el cumplimiento de sus funciones y responsabilidades, proporcionándole un análisis objetivo, evaluaciones y recomendaciones pertinentes sobre las operaciones examinadas.

Otros objetivos que se busca concretar a través de la auditoría interna son: realizar investigaciones especiales solicitadas por la dirección, preparar informes de auditoría acerca de las irregularidades que pudiesen encontrarse como resultado de las investigaciones, expresando igualmente las recomendaciones que se juzguen adecuadas, vigilar el cumplimiento de la recomendaciones contenidas en los informes emitidos con anterioridad.

La auditoría interna posee varias ventajas: facilita una ayuda primordial a la dirección al evaluar de forma relativamente independiente los sistemas de organización y de administración, facilita una evaluación global y objetiva de los problemas de la empresa que generalmente suelen ser interpretados de una manera parcial por los departamentos afectados, pone a disposición de la dirección un profundo conocimiento de las operaciones de la empresa, proporcionado por el trabajo de verificación de los datos contables y financieros, contribuye eficazmente a evitar las actividades rutinarias que generalmente se desarrollan en las grandes empresas, favorece la protección de los intereses y bienes de la empresa frente a terceros.

2.2.2 Auditoría externa. Se puede definir como los métodos empleados por una firma externa, los objetivos de la auditoría externa son: proporcionar a la dirección y a los propietarios de la empresa unos estados financieros certificados por una autoridad independiente e imparcial, proporcionar asesoramiento a la gerencia y a los responsables de las distintas áreas de la empresa en materia de sistemas contables y financieros, procedimientos de organización y otras numerosas fases de la operatoria de una empresa, suministrar información objetiva que sirva de base a las entidades de información y clasificación crediticia, servir de punto de partida en las negociaciones para la compraventa de las acciones de una empresa, reducir y controlar riesgos accidentales, fraudes y otras actuaciones anormales, liberar implícitamente a la gerencia de sus responsabilidades de gestión.

2.2.3 Auditoria de sistemas. Dirigida a evaluar los sistemas y procedimientos de uso en una empresa, con el propósito de determinar si su diseño y aplicación son correctos; y comprobar el sistema de procesamiento de información como parte de la evaluación de control interno; así como para identificar aspectos susceptibles de mejorarse o eliminarse.

2.2.4 Auditoria informática. La auditoría informática es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. Permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos.[2]

[2] http://www.gerencie.com/auditoria-de-sistemas-de-informacion.html

2.4 AUDITORIA DE SISTEMAS COMO OBJETO DE ESTUDIO

La auditoría de sistemas es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. También permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes.

Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos. Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

La auditoría de sistemas permite además verificar que la información desde su entrada, procedimientos, controles, almacenamientos y salidas, sea integra y verificable y por tanto permita el apoyo a la toma de decisiones dentro de una organización.

Dentro de este procedimiento es necesario evaluar los mecanismos de control implantados en una organización, determinando así, si son adecuados y cumplen con los objetivos o estrategias, de esta manera, es posible proponer cambios que se deberían realizar para el mejoramiento de los mismos. Estos mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

2.4.1 Alcance de la auditoria de sistemas. El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoría de sistemas, se complementa con los objetivos de ésta. El alcance ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas. La indefinición de los alcances de la auditoria compromete el éxito o el fracaso de la misma. Así mismo, las personas que realizan la auditoría han de conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar[3].

[3] http://www.buenastareas.com/ensayos/Tipos-De-Auditoria/1468357.html

2.4.2 Objetivos de la auditoria de sistemas:

- **Objetivo general de la auditoria de sistemas**

El objetivo principal de la auditoria de sistemas es evaluar el uso adecuado de los sistemas para el correcto ingreso de datos, el procesamiento adecuado de la información y la emisión oportuna de los resultados en la organización, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas de información dentro de la empresa.

- **Objetivos específicos de la auditoria de sistemas**

✓ El control de la función informática.
✓ El análisis de la eficiencia de los Sistemas Informáticos.
✓ La verificación del cumplimiento de la Normativa en este ámbito.
✓ La revisión de la eficaz gestión de los recursos informáticos.

La auditoría de sistemas sirve para mejorar ciertas características en la empresa como:

✓ Eficiencia
✓ Eficacia
✓ Rentabilidad
✓ Seguridad

2.4.3 Principales pruebas y herramientas para efectuar una auditoría de sistemas:

- **Pruebas sustantivas:** Verifican el grado de confiabilidad del sistema de información de la organización. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican así mismo la exactitud, integridad y validez de la información.

- **Pruebas de cumplimiento:** Verifican el grado de cumplimiento de aquello extraído el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente

Las principales herramientas de las que dispone un auditor informático son:

- Observación
- Realización de cuestionarios

- Entrevistas a auditados y no auditados
- Muestreo estadístico
- Flujo gramas
- Listas de chequeo
- Mapas conceptuales

2.4.4 Perfiles Profesionales de los auditores informáticos:

Tabla 1: Perfiles profesionales y actividades

Experto en Bases de Datos y Administración de las mismas.	Con experiencia en el mantenimiento de Bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación
Experto en Software de Comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Muy experto en Subsistemas de teleproceso.
Experto en Explotación y Gestión de CPD´S	Responsable de algún Centro de Cálculo. Amplia experiencia en Automatización de trabajos. Experto en relaciones humanas. Buenos conocimientos de los sistemas.
Técnico de Organización	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
Técnico de evaluación de Costes	Economista con conocimiento de Informática. Gestión de costes.

Experto en Bases de Datos y Administración de las mismas.	Con experiencia en el mantenimiento de Bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación
Experto en Software de Comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Muy experto en Subsistemas de teleproceso.
Experto en Explotación y Gestión de CPD´S	Responsable de algún Centro de Cálculo. Amplia experiencia en Automatización de trabajos. Experto en relaciones humanas. Buenos conocimientos de los sistemas.
Técnico de Organización	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
Técnico de evaluación de Costes	Economista con conocimiento de Informática. Gestión de costes.

2.4.5 Pasos a seguir para una auditoria de sistemas en una organización:

Estudio preliminar: Para realizar dicho estudio se examinan las funciones y actividades generales del área o departamento de sistemas, con el fin de tener un contacto inicial con el personal de dicha área, y conocer a grandes rasgos la distribución del sistema, características de equipos, instalaciones y medidas de seguridad visibles.

Para su realización el auditor debe conocer lo siguiente:

- **Organización:** Es de vital importancia conocer dentro del departamento o área de sistemas quien es el jefe, quien diseña y quien ejecuta, para lo cual es necesario conocer:

  - Organigrama: El organigrama permite conocer la estructura oficial dentro de la organización a auditar.

  - Departamentos: Es importante conocer los departamentos que hacen parte de la organización y las funciones que se deben llevar a cabo dentro de cada uno de ellos.

  - Relaciones Jerárquicas y funcionales entre órganos de la Organización: Es necesario verificar si dentro de la organización se cumplen las relaciones funcionales y jerárquicas que se evidencian dentro del organigrama.

- **Corrientes de información:** Los flujos de información entre los diferentes departamentos dentro de una organización son de vital importancia ya que evidencian una gestión eficiente, siempre y cuando estas corrientes no vayan en direcciones no contempladas dentro del organigrama.

  En muchas ocasiones es posible que se hayan creado canales de información alternativos, lo cual ocurre cuando existen pequeños o grandes fallos en la estructura de la organización.

  Además, la aparición de corrientes de información no planeados pueden obedecer a afinidades personales o desacato a las reglas establecidas. Los cuales pueden producir perturbaciones dentro de la organización.

- **Flujos de información:** Dentro del proceso de auditoría es necesario verificar que los nombres de los cargos dentro de la organización correspondan a las funciones que realiza esa persona. Puede ocurrir que bajo nombres de cargos diferentes se realicen funciones idénticas, en este caso se estaría realizando tareas redundantes lo cual podría conllevar a deficiencias estructurales.

- **Entorno operacional:** Es importante conocer por parte de los auditores de sistemas la referencia del entorno en el cual se va a trabajar, esto se logra determinando:

  - Ubicación geográfica del o los centros de procesamiento de información de la empresa. Evaluando además el personal responsable de cada uno de ellos.

  - Arquitectura y configuración de Hardware y Software: es fundamental la verificación de la compatibilidad e intercomunicación de los equipos ya que estas, están estrechamente ligadas a los grados de seguridad lógica de las organizaciones[4].

  - Situación geográfica de los sistemas: el equipo auditor debe estudiar la información que proporcione la organización sobre los elementos físicos y lógicos de las instalaciones.

Comunicación y Redes de Comunicación: se debe disponer de un inventario, estado y características de las redes de comunicación.

- **Aplicaciones bases de datos:** Finalmente para el equipo auditor es necesario tener una idea general de los procesos informáticos realizados dentro de la organización.

Para ello es necesario recolectar la siguiente información:

  - Inventario de Hardware y Software

  - Volumen, antigüedad y complejidad de las aplicaciones

Se clasificará globalmente la existencia total o parcial de metodología en el desarrollo de las aplicaciones.

Si se han utilizados varias a lo largo del tiempo se pondrá de manifiesto:

  - Metodología del diseño: La existencia de una adecuada documentación de las aplicaciones proporciona beneficios tangibles e inmediatos muy importantes.

La documentación de programas disminuye gravemente el mantenimiento de los mismos.

  - Documentación: El auditor recaudara información de tamaño y características de las Bases de Datos, clasificándolas en relación y jerarquías. Hallará un promedio de número de accesos a ellas por hora o días. Esta operación se

[4] PIATTINI, Mario y Emilio del Peso. Auditoría Informática. Un enfoque práctico. Editorial RA-MA.

repetirá con los ficheros, así como la frecuencia de actualizaciones de los mismos.

Estos datos proporcionan una visión aceptable de las características de la carga informática.

- **Determinación de recursos de la auditoría de sistemas.** Por medio de los resultados del estudio preliminar es posible determinar los recursos humanos y físicos que son necesarios en el proceso de auditoría.

- **Elaboración del plan y de los programas de trabajo.** El plan de trabajo se realiza de acuerdo a los siguientes criterios:

➢ El proceso de auditoría se llevara a cabo en áreas generales o específicas.

➢ La auditoría se hará de manera global o especifica.

➢ De acuerdo a si se manejaran recursos genéricos o específicos se realizará un cronograma de trabajo.

➢ El Plan establece disponibilidad futura de los recursos durante la revisión.

➢ El Plan estructura las tareas a realizar por cada integrante del grupo auditoria.

➢ En el Plan se expresan todas las ayudas que el auditor ha de recibir del auditado.

Una vez elaborado el Plan, se procede a la Programación de actividades, esta ha de ser lo suficientemente flexible como para permitir modificaciones a lo largo del proyecto.

- **Actividades de la auditoría de sistemas.** La auditoría de sistemas general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos.

Cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente y con menor calidad.

➢ **Técnicas de trabajo:**

- Análisis de la información recabada del auditado
- Análisis de la información propia

- Cruzamiento de las informaciones anteriores
- Entrevistas
- Simulación
- Muestreos

- **Herramientas:**

- Cuestionario general inicial
- Cuestionario Checklist
- Estándares
- Monitores
- Simuladores (Generadores de datos)
- Paquetes de auditoría (Generadores de programas)
- Matrices de riesgo

- **Informe final.** El informe final de la auditoria de sistemas se realiza por escrito, el cual contempla la siguiente estructura:

- Definición de objetivos y alcance de la auditoría
- Enumeración de temas objeto de la auditoria
- Cuerpo de la auditoria: para lo cual se mostrara los siguiente para cada tema:

- Situación actual
- Tendencias futuras
- Puntos débiles y amenazas
- Recomendaciones y planes de acción
- Redacción posterior de la carta de introducción o presentación

Algunas características que deben ser consideradas en los informes, son:
Las características de fondo se refieren a que la información sea veraz y oportuna, el uso de la terminología se exacta y objetiva, que exista congruencia con lo observado sin hacer ninguna distorsión de lo encontrado.

Las características de forma: el estilo de redacción concreto conciso, clara, sencilla y amena, que no haya redundancia, redacción impecable en ortografía.

2.5 METODOLOGÍAS DE AUDITORIA DE SISTEMAS

La auditoría de sistemas en el ámbito empresarial, ha sido de gran importancia, puesto que con ella se pretende gestionar la información y sirve como apoyo a la toma de decisiones. Además se busca disponer de un sistema de información que sea eficiente y eficaz para obtener la mayor productividad y calidad posibles, debido a que la información se ha convertido en el activo más importante de las empresas.

En la actualidad, gran parte de las organizaciones consideran que la información y la tecnología representan activos importantes para la misma, sin dejar de lado otros activos indispensables, como los requerimientos de calidad, controles, seguridad e información. Por tal razón los directivos deben establecer un adecuado sistema de control interno, para proporcionar seguridad razonable, respecto a si están lográndose los objetivos como: promover la efectividad y eficiencia de las operaciones, proteger y conservar todos los recursos de la organización, cumplir las leyes y reglamentos internos y externos relacionados con la empresa.

Para esto, se hace necesario aplicar una auditoria de sistemas llevando a cabo una metodología adecuada, que permita evaluar de manera objetiva las vulnerabilidades o falta de controles existentes en la empresa.

Las metodologías desarrolladas y utilizadas en la auditoría y el control informático, se dividen en dos grupos:

- Cuantitativas
- Cualitativas

Las metodologías cuantitativas están basadas en un modelo matemático, diseñadas para producir una lista de riesgos que pueden compararse entre sí con facilidad por tener asignados unos valores numéricos. Estos valores son datos de probabilidad de ocurrencia de un evento que se debe extraer de un riesgo de incidencias donde el número de incidencias tiende al infinito.

Y las metodologías cualitativas están basadas en el criterio humano capaz de definir un proceso de trabajo. Así mismo, esta metodología establece métodos estadísticos y lógica borrosa, que requiere menos recursos humanos y menos tiempo que las metodologías cuantitativas.

Esta metodología presenta un enfoque amplio y logra un plan de trabajo flexible y reactivo. Sin embargo tiene la desventaja de depender mucho de la experiencia, habilidad y calidad del profesional involucrado. Dicha anomalía nace de la dificultad que tiene un profesional sin experiencia que asume la función auditora y busca una fórmula fácil que le permita empezar su trabajo rápidamente. Por lo tanto es necesario que el auditor tenga una gran experiencia y una gran formación tanto auditora como informática. Esta formación debe ser adquirida mediante el estudio y la práctica.

Estas últimas hacen parte de los modelos a seguir dentro del control interno y son necesarias para desarrollar cualquier proyecto de manera ordenada y eficaz, por lo que cada una cumple un papel importante y al optar por una de ellas, el auditor debe cumplirlas a cabalidad.

2.5.1 COBIT (Control objectives for information and related technology:

La Organización ISACA (Information Systems Audit and Control Association), se formó como una fundación de educación para llevar a cabo los esfuerzos de investigación a gran escala para expandir el conocimiento y el valor de la gobernanza de las Tecnologías de Información (TI) y el campo de control. A través de su Fundación, publicó en 1995 el COBIT, como resultado de cuatro años de intensa investigación.

El COBIT es una metodología utilizada en las empresas para auditar los sistemas de información, donde se evalúa la gestión y el control, enfocado a los administradores de las TI, los usuarios y los auditores encargados del proceso.
COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos, esta 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.
En la auditoria de sistemas existen varias metodologías como: COBIT (ISACA), COSO, SAC, AICPA (SAS), IFAC (NIA), MARGERIT y EDP. Sin embargo, las metodologías más utilizadas son: COBIT y COSO.

La estructura del modelo COBIT evalúa los criterios de información, como la seguridad y calidad, así como también se verifican los recursos que comprenden la tecnología de información, como el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos implicados en la organización.

Cuando se implementa el COBIT adecuadamente en una organización, se evalúa de manera ágil y consistente el cumplimiento de los objetivos de control, haciendo que los procesos y recursos de información y tecnología contribuyan al logro de los objetivos de la empresa.

El modelo COBIT, clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro dominios:

- **Dominio: Planificación y organización (PO).**

Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos de negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

Procesos:

- **PO1 Definición de un plan estratégico**

  - PO1.1 Administración del valor de TI
  - PO1.2 Alineación de TI con el negocio
  - PO1.3 Evaluación del desempeño y la capacidad actual
  - PO1.4 Plan estratégico de TI
  - PO1.5 Planes tácticos de TI
  - PO1.6 Administración del portafolio de TI

Objetivo: Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar sus logros futuros.

Su realización se concreta a través un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo, los que deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo, teniendo en cuenta:

- **PO2 Definición de la arquitectura de información**

  - PO2.1 Modelo de arquitectura de información empresarial
  - PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos
  - PO2.3 Esquema de clasificación de datos
  - PO2.4 Administración de integridad

Objetivo: Satisfacer los requerimientos de negocio, organizando de la mejor manera posible los sistemas de información, a través de la creación y mantenimiento de un modelo de información de negocio, asegurándose que se definan los sistemas apropiados para optimizar la utilización de esta información, tomando en consideración[5]:

- La documentación deberá conservar consistencia con las necesidades permitiendo a los responsables llevar a cabo sus tareas eficiente y oportunamente.

- El diccionario de datos, el cual incorporara las reglas de sintaxis de datos de la organización y deberá ser continuamente actualizado.

[5] Tesis, Auditoria al módulo de historia clínica. Jenny Burgos y Carolina Domínguez. Año 2007. Pág. 59-60 y 87-94

- **PO3 Determinación de la dirección tecnológica**

  - PO3.1 Planeación de la dirección tecnológica
  - PO3.2 Plan de infraestructura tecnológica
  - PO3.3 Monitoreo de tendencias y regulaciones futuras
  - PO3.4 Estándares tecnológicos
  - PO3.5 Consejo de arquitectura de TI

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

- La capacidad de adecuación y evolución de la infraestructura actual, que deberá concordar con los planes a largo y corto plazo de tecnología de información y debiendo abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.

- El monitoreo de desarrollos tecnológicos que serán tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.

- Planes de adquisición, los cuales deberán reflejar las necesidades identificadas en el plan de infraestructura tecnológica.

- **PO4 Definición de la organización y de las relaciones de TI**

  - PO4.1 Marco de trabajo de procesos de TI
  - PO4.2 Comité estratégico de TI
  - PO4.3 Comité directivo de TI
  - PO4.4 Ubicación organizacional de la función de TI
  - PO4.5 Estructura organizacional
  - PO4.6 Establecimiento de roles y responsabilidades
  - PO4.7 Responsabilidad de aseguramiento de calidad de TI
  - PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento
  - PO4.9 Propiedad de datos y de sistemas
  - PO4.10 Supervisión
  - PO4.11 Segregación de FUNCIONES
  - PO4.12 Personal de TI
  - PO4.13 Personal clave de TI
  - PO4.14 Políticas y procedimientos para personal contratado
  - PO4.15 Relaciones

Objetivo: Prestación de servicios de TI

Esto se realiza por medio de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas, teniendo en cuenta:

- El comité de dirección el cual se encargara de vigilar la función de servicios de información y sus actividades.

- Propiedad, custodia, la Gerencia deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades deberán estar claramente definidas.

- Supervisión, para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente

- Segregación de funciones, con la que se evitará la posibilidad de que un solo individuo resuelva un proceso crítico.

➢ **PO5 Manejo de la inversión**

- PO5.1 Marco de trabajo para la administración financiera
- PO5.2 Prioridades dentro del presupuesto de TI
- PO5.3 Proceso presupuestal
- PO5.4 Administración de costos de TI
- PO5.5 Administración de beneficios

Objetivo: tiene como finalidad la satisfacción de los requerimientos de negocio, asegurando el financiamiento y el control de desembolsos de recursos financieros. Su realización se concreta a través presupuestos periódicos sobre inversiones y operaciones establecidas y aprobados por el negocio, teniendo en cuenta:

- Las alternativas de financiamiento, se deberán investigar diferentes alternativas de financiamiento.

- El control del gasto real, se deberá tomar como base el sistema de contabilidad de la organización, mismo que deberá registrar, procesar y reportar rutinariamente los costos asociados con las actividades de la función de servicios de información

- La justificación de costos y beneficios, deberá establecerse un control gerencial que garantice que la prestación de servicios por parte de la función de servicios de información se justifique en cuanto a costos. Los beneficios derivados de las actividades de TI deberán ser analizados en forma similar.

- **PO6 Comunicación de la dirección y aspiraciones de la gerencia**

  - PO6.1 Ambiente de políticas y de control
  - po6.2 riesgo corporativo y marco de referencia de control interno de TI
  - PO6.3 Administración de políticas para TI
  - PO6.4 Implantación de políticas de TI
  - PO6.5 Comunicación de los objetivos y la dirección de TI

Objetivo: Asegura el conocimiento y comprensión de los usuarios sobre las aspiraciones del alto nivel (gerencia), se concreta a través de políticas establecidas y transmitidas a la comunidad de usuarios, necesitándose para esto estándares para traducir las opciones estratégicas en reglas de usuario prácticas y utilizables. Toma en cuenta:

- Los código de ética / conducta, el cumplimiento de las reglas de ética, conducta, seguridad y estándares de control interno deberá ser establecido por la Alta Gerencia y promoverse a través del ejemplo.
- Las directrices tecnológicas

- El cumplimiento, la Gerencia deberá también asegurar y monitorear la duración de la implementación de sus políticas.

- El compromiso con la calidad, la Gerencia de la función de servicios de información deberá definir, documentar y mantener una filosofía de calidad, debiendo ser comprendidos, implementados y mantenidos por todos los niveles de la función de servicios de información.

- **PO7 Administración de recursos humanos**

  - PO7.1 Reclutamiento y retención del personal
  - PO7.2 Competencias del personal
  - PO7.3 Asignación de roles
  - PO7.4 Entrenamiento del personal de TI
  - PO7.5 Dependencia sobre los individuos
  - PO7.6 Procedimientos de investigación del personal
  - PO7.7 Evaluación del desempeño del empleado
  - PO7.8 Cambios y terminación de trabajo

Objetivo: Maximizar las contribuciones del personal a los procesos de TI, satisfaciendo así los requerimientos de negocio, a través de técnicas sólidas para administración de personal, tomando en consideración:

- El reclutamiento y promoción, deberá tener como base criterios objetivos, considerando factores como la educación, la experiencia y la responsabilidad.

- Los requerimientos de calificaciones, el personal deberá estar calificado, tomando como base una educación, entrenamiento y o experiencia apropiados, según se requiera.

- La capacitación, los programas de educación y entrenamiento estarán dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal.

➢ **PO8 Asegurar el cumplimiento con los requerimientos externos**

Objetivo: Cumplir con obligaciones legales, regulatorias y contractuales. Para ello se realiza una identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, llevando a cabo las medidas apropiadas para cumplir con ellos y se toma en consideración:

- Definición y mantenimiento de procedimientos para la revisión de requerimientos externos, para la coordinación de estas actividades y para el cumplimiento continúo de los mismos.
- Leyes, regulaciones y contratos

- Revisiones regulares en cuanto a cambios

- Búsqueda de asistencia legal y modificaciones

- Seguridad y ergonomía con respecto al ambiente de trabajo de los usuarios y el personal de la función de servicios de información.

- Privacidad

- Propiedad intelectual

- Flujo de datos externos y criptografía

➢ **PO9 Evaluación de riesgos**

- PO9.1 Marco de trabajo de administración de riesgos
- PO9.2 Establecimiento del contexto del riesgo
- PO9.3 Identificación de eventos
- PO9.4 Evaluación de riesgos de TI
- PO9.5 Respuesta a los riesgos
- PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos

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

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

- Identificación, definición y actualización regular de los diferentes tipos de riesgos de TI (por ej.: tecnológicos, de seguridad, etc.) de manera de que se pueda determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable.

- Definición de alcances, límites de los riesgos y la metodología para las evaluaciones de los riesgos.

- Actualización de evaluación de riesgos.

- Metodología de evaluación de riesgos.

- Medición de riesgos cualitativos y/o cuantitativos

➢ **PO10 Administración de proyectos**

- PO10.1 Marco de trabajo para la administración de programas
- PO10.2 Marco de trabajo para la administración de proyectos
- PO10.3 Enfoque de administración de proyectos
- PO10.4 Compromiso de los interesados
- PO10.5 Declaración de alcance del proyecto
- PO10.6 Inicio de las fases del proyecto
- PO10.7 Plan integrado del proyecto
- PO10.8 Recursos del proyecto
- PO10.9 Administración de riesgos del proyecto
- PO10.10 Plan de calidad del proyecto
- PO10.11 Control de cambios del proyecto
- PO10.12 Planeación del proyecto y métodos de aseguramiento
- PO10.13 Medición del desempeño, reporte y monitoreo del proyecto
- PO10.14 Cierre del proyecto

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

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

- Definición de un marco de referencia general para la administración de proyectos que defina el alcance y los límites del mismo, así como la metodología de administración de proyectos a ser adoptada y aplicada para cada proyecto emprendido. La metodología deberá cubrir, como mínimo, la asignación de responsabilidades, la determinación de tareas, la realización de presupuestos de tiempo y recursos, los avances, los puntos de revisión y las aprobaciones.

- El involucramiento de los usuarios en el desarrollo, implementación o modificación de los proyectos.

➢ **PO11 Administración de calidad**

- PO8.1 Sistema de administración de calidad
- PO8.2 Estándares y prácticas de calidad
- PO8.3 Estándares de desarrollo y de adquisición
- PO8.4 Enfoque en el cliente de TI
- PO8.5 Mejora continua
- PO8.6 Medición, monitoreo y revisión de la calidad.

Objetivo: Satisfacer los requerimientos del cliente. Para ello se realiza una planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización y se toma en consideración:

- Definición y mantenimiento regular del plan de calidad, el cual deberá promover la filosofía de mejora continua y contestar a las preguntas básicas de qué, quién y cómo.

- Responsabilidades de aseguramiento de calidad que determine los tipos de actividades de aseguramiento de calidad tales como revisiones, auditorias, inspecciones, etc. que deben realizarse para alcanzar los objetivos del plan general de calidad.

- **Dominio: Adquisición e implementación.**

Para llevar a cabo la estrategia de TI, las soluciones de Ti deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.
Procesos:

➢ **AI1 Identificación de soluciones automatizadas**

- AI1.1 Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio

- AI1.2 Reporte de análisis de riesgos
- AI1.3 Estudio de factibilidad y formulación de cursos de acción alternativos
- AI1.4 Requerimientos, decisión de factibilidad y aprobación

Objetivo: Asegurar el mejor enfoque para cumplir con los requerimientos del usuario.

Para ello se realiza un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios y toma en consideración:

- Definición de requerimientos de información para poder aprobar un proyecto de desarrollo.

- Estudios de factibilidad con la finalidad de satisfacer los requerimientos del negocio establecidos para el desarrollo de un proyecto.

- Arquitectura de información para tener en consideración el modelo de datos al definir soluciones y analizar la factibilidad de las mismas.

➢ **AI2 Adquisición y mantenimiento del software aplicativo**

- AI2.1 Diseño de alto nivel
- AI2.2 Diseño detallado
- AI2.3 Control y posibilidad de auditar las aplicaciones
- AI2.4 Seguridad y disponibilidad de las aplicaciones
- AI2.5 Configuración e implantación de software aplicativo adquirido
- AI2.6 Actualizaciones importantes en sistemas existentes
- AI2.7 Desarrollo de software aplicativo
- AI2.8 Aseguramiento de la calidad del software
- AI2.9 Administración de los requerimientos de aplicaciones
- AI2.10 Mantenimiento de software aplicativo

Objetivo: Proporciona funciones automatizadas que soporten efectivamente al negocio.

Para ello se definen declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros y se toma en consideración:

- Requerimientos de usuarios, para realizar un correcto análisis y obtener un software claro y fácil de usar.

- Requerimientos de archivo, entrada, proceso y salida.

- Interface usuario-maquina asegurando que el software sea fácil de utilizar y que sea capaz de auto documentarse.

- Realizar pruebas funcionales (unitarias, de aplicación, de integración y de carga y estrés), de acuerdo con el plan de prueba del proyecto y con los estándares establecidos antes de ser aprobado por los usuarios.

➢ **AI3 Adquisición y mantenimiento de la infraestructura tecnológica**

- AI3.1 Plan de adquisición de infraestructura tecnológica
- AI3.2 Protección y disponibilidad del recurso de infraestructura
- AI3.3 Mantenimiento de la infraestructura
- AI3.4 Ambiente de prueba de factibilidad

Objetivo: Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios.

Para ello se realizara una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema y toma en consideración:

- Evaluación de tecnología para identificar el impacto del nuevo hardware o software sobre el rendimiento del sistema general.

- Mantenimiento preventivo del hardware con el objeto de reducir la frecuencia y el impacto de fallas de rendimiento.

- Seguridad del software de sistema, instalación y mantenimiento para no arriesgar la seguridad de los datos y programas ya almacenados en el mismo.

➢ **AI4 Desarrollo y mantenimiento de procedimientos**

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

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

- Manuales de procedimientos de usuarios y controles, de manera que los mismos permanezcan en permanente actualización para el mejor desempeño y control de los usuarios.

- Manuales de Operaciones y controles, de manera que estén en permanente actualización.

- Materiales de entrenamiento enfocados al uso del sistema en la práctica diaria.

➢ **AI5 Instalación y aceptación de los sistemas**

- AI7.1 Entrenamiento
- AI7.2 Plan de prueba
- AI7.3 Plan de implantación
- AI7.4 Ambiente de prueba
- AI7.5 Conversión de sistemas y datos
- AI7.6 Pruebas de cambios
- AI7.7 Prueba de aceptación final.
- AI7.8 Promoción a producción
- AI7.9 Revisión posterior a la implantación

Objetivo: Verificar y confirmar que la solución sea adecuada para el propósito deseado

Para ello se realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas y toma en consideración:

- Capacitación del personal de acuerdo al plan de entrenamiento definido y los materiales relacionados.

- Conversión / carga de datos, de manera que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo.

- Pruebas específicas (cambios, desempeño, aceptación final, operacional) con el objeto de obtener un producto satisfactorio.

➢ **AI6 Administración de los cambios**

- AI6.1 Estándares y procedimientos para cambios
- AI6.2 Evaluación de impacto, priorización y autorización
- AI6.3 Cambios de emergencia
- AI6.4 Seguimiento y reporte del estatus de cambio
- AI6.5 Cierre y documentación del cambio

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

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

- Identificación de cambios tanto internos como por parte de proveedores

- Procedimientos de categorización, priorización y emergencia de solicitudes de cambios.

- Evaluación del impacto que provocaran los cambios.

- Autorización de cambios

- Manejo de liberación de manera que la liberación de software este regida por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega, etc.

- **Dominio: Entregar y dar soporte.**

En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

Procesos:

- **DS1 Definición de niveles de servicio**

  - DS1.1 Marco de trabajo de la administración de los niveles de servicio
  - DS1.2 Definición de servicios
  - DS1.3 Acuerdos de niveles de servicio
  - DS1.4 Acuerdos de niveles de operación
  - DS1.5 Monitoreo y reporte del cumplimento de los niveles de servicio
  - DS1.6 Revisión de los acuerdos de niveles de servicio y de los contratos

Objetivo: Establecer una comprensión común del nivel de servicio requerido
Para ello se establecen convenios de niveles de servicio que formalicen los criterios de desempeño contra los cuales se medirá la cantidad y la calidad del servicio y se toma en consideración:

- Convenios formales que determinen la disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia / recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio.

- Definición de las responsabilidades de los usuarios y de la función de servicios de información.

- **DS2 Administración de servicios prestados por terceros**

  - DS2.1 Identificación de todas las relaciones con proveedores
  - DS2.2 Gestión de relaciones con proveedores
  - DS2.3 Administración de riesgos del proveedor
  - DS2.4 Monitoreo del desempeño del proveedor

Objetivo: Asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos

Para ello se establecen medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización y toma en consideración:

- Acuerdos de servicios con terceras partes a través de contratos entre la organización y el proveedor de la administración de instalaciones este basado en niveles de procesamiento requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones según sea apropiado.

- Acuerdos de confidencialidad. Además, se deberá calificar a los terceros y el contrato deberá definirse y acordarse para cada relación de servicio con un proveedor.

- **DS3 Administración de desempeño y capacidad**

  - DS3.1 Planeación del desempeño y la capacidad
  - DS3.2 Capacidad y desempeño actual
  - DS3.3 Capacidad y desempeño futuros
  - DS3.4 Disponibilidad de recursos de TI
  - DS3.5 Monitoreo y reporte

Objetivo: Asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado.

Para ello se realizan controles de manejo de capacidad y desempeño que recopilen datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos y toma en consideración:

- Requerimientos de disponibilidad y desempeño de los servicios de sistemas de información

- Monitoreo y reporte de los recursos de tecnología de información.

- Utilizar herramientas de modelado apropiadas para producir un modelo del sistema actual para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de configuración, desempeño y disponibilidad.

➢ **DS4 Asegurar el servicio continuo**

- DS4.1 Marco de trabajo de continuidad de TI
- DS4.2 Planes de continuidad de TI
- DS4.3 Recursos críticos de TI
- DS4.4 Mantenimiento del plan de continuidad de TI
- DS4.5 Pruebas del plan de continuidad de TI
- DS4.6 Entrenamiento del plan de continuidad de TI
- DS4.7 Distribución del plan de continuidad de TI
- DS4.8 Recuperación y reanudación de los servicios de TI
- DS4.9 Almacenamiento de respaldos fuera de las instalaciones
- DS4.10 Revisión post reanudación

Objetivo: mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones. Para ello se tiene un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio y toma en consideración:

- Planificación de severidad
- Plan documentado
- Procedimientos alternativos
- Respaldo y recuperación
- Pruebas y entrenamiento sistemático y singulares

➢ **DS5 Garantizar la seguridad de sistemas**

- DS5.1 Administración de la seguridad de TI
- DS5.2 Plan de seguridad de TI
- DS5.3 Administración de identidad
- DS5.4 Administración de cuentas del usuario
- DS5.5 Pruebas, vigilancia y monitoreo de la seguridad
- DS5.6 Definición de incidente de seguridad
- DS5.7 Protección de la tecnología de seguridad
- DS5.8 Administración de llaves criptográficas
- DS5.9 Prevención, detección y corrección de software malicioso
- DS5.10 Seguridad de la red
- DS5.11 Intercambio de datos sensitivos

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

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

- Autorización, autenticación y el acceso lógico junto con el uso de los recursos de TI deberá restringirse a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso

- Perfiles e identificación de usuarios estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario

➢ **DS6 Educación y entrenamiento de usuarios**

- DS6.1 Identificación de Necesidades de Entrenamiento y Educación
- DS6.2 Impartición de Entrenamiento y Educación
- DS6.3 Evaluación del Entrenamiento Recibido

Objetivo: Asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados.
Para ello se realiza un plan completo de entrenamiento y desarrollo y se toma en consideración:

- Currículo de entrenamiento estableciendo y manteniendo procedimientos para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información
- Campañas de concientización, definiendo los grupos objetivos, identificar y asignar entrenadores y organizar oportunamente las sesiones de entrenamiento

- Técnicas de concientización proporcionando un programa de educación y entrenamiento que incluya conducta ética de la función de servicios de información

➢ **DS7 Identificación y asignación de costos**

- DS7.1 Definición de Servicios
- DS7.2 Contabilización de TI
- DS7.3 Modelación de Costos y Cargos
- DS7.4 Mantenimiento del Modelo de Costos

Objetivo: Asegurar un conocimiento correcto de los costos atribuibles a los servicios de TI

Para ello se realiza un sistema de contabilidad de costos que asegure que éstos sean registrados, calculados y asignados a los niveles de detalle requeridos y toma en consideración:

- Los elementos sujetos a cargo deben ser recursos identificables, medibles y predecibles para los usuarios

- Procedimientos y políticas de cargo que fomenten el uso apropiado de los recursos de cómputo y aseguren el trato justo de los departamentos usuarios y sus necesidades

➢ **DS8 Apoyo y asistencia a los clientes de TI**

Objetivo: asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente

Para ello se realiza un Buró de ayuda que proporcione soporte y asesoría de primera línea y toma en consideración:

- Consultas de usuarios y respuesta a problemas estableciendo un soporte de una función de buró de ayuda

- Monitoreo de consultas y despacho estableciendo procedimientos que aseguren que las preguntas de los clientes que pueden ser resueltas sean reasignadas al nivel adecuado para atenderlas

- Análisis y reporte de tendencias adecuado de las preguntas de los clientes y su solución, de los tiempos de respuesta y la identificación de tendencias

➢ **DS9 Administración de la configuración**

- DS9.1 Repositorio y línea base de configuración
- DS9.2 Identificación y mantenimiento de elementos de configuración
- DS9.3 Revisión de integridad de la configuración

Objetivo: Dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios

Para ello se realizan controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia y toma en consideración:

- Registro de activos estableciendo procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, al momento de adquisición

- Administración de cambios en la configuración asegurando que los registros de configuración reflejen el status real de todos los elementos de la configuración

➢ **DS10 Administración de problemas**

- DS10.1 Identificación y clasificación de problemas
- DS10.2 Rastreo y resolución de problemas
- DS10.3 Cierre de problemas
- DS10.4 Integración de las administraciones de cambios, configuración y problemas

Objetivo: Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder.

Para ello se necesita un sistema de manejo de problemas que registre y dé seguimiento a todos los incidentes, además de un conjunto de procedimientos de escalamiento de problemas para resolver de la manera más eficiente los problemas identificados. Este sistema de administración de problemas deberá también realizar un seguimiento de las causas a partir de un incidente dado.

➢ **DS11 Administración de datos**

- DS11.1 Requerimientos del Negocio para Administración de Datos
- DS11.2 Acuerdos de Almacenamiento y Conservación
- DS11.3 Sistema de Administración de Librerías de Medios
- DS11.4 Eliminación
- DS11.5 Respaldo y Restauración
- DS11.6 Requerimientos de Seguridad para la Administración de Datos

Objetivo: Asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento.

Lo cual se logra a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI. Para tal fin, la gerencia deberá diseñar formatos de entrada de datos para los usuarios de manera que se minimicen lo errores y las omisiones durante la creación de los datos.

Este proceso deberá controlar los documentos fuentes (de donde se extraen los datos), de manera que estén completos, sean precisos y se registren apropiadamente. Se deberán crear también procedimientos que validen los datos de entrada y corrijan o detecten los datos erróneos, como así también

procedimientos de validación para transacciones erróneas, de manera que éstas no sean procesadas. Cabe destacar la importancia de crear procedimientos para el almacenamiento, respaldo y recuperación de datos, teniendo un registro físico (discos, disquetes, CDs y cintas magnéticas) de todas las transacciones y datos manejados por la organización, albergados tanto dentro como fuera de la empresa.

La gerencia deberá asegurar también la integridad, autenticidad y confidencialidad de los datos almacenados, definiendo e implementando procedimientos para tal fin.

- **DS12 Administración de las instalaciones**

  - DS12.1 Selección y diseño del centro de datos
  - DS12.2 Medidas de seguridad física
  - DS12.3 Acceso físico
  - DS12.4 Protección contra factores ambientales
  - DS12.5 Administración de instalaciones físicas

Objetivo: Proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

- **DS13 Administración de la operación**

  - DS13.1 Procedimientos e instrucciones de operación
  - DS13.2 Programación de tareas
  - DS13.3 Monitoreo de la infraestructura de TI
  - DS13.4 Documentos sensitivos y dispositivos de salida
  - DS13.5 Mantenimiento preventivo del hardware

Objetivo: Asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada.

Esto se logra a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, la gerencia deberá establecer y documentar procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales deberán ser revisados periódicamente para garantizar su eficiencia y cumplimiento.

- **Dominio: Monitorear y evaluar.**

Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad. Este es, precisamente, el ámbito de este dominio.

Procesos

- **M1 Monitoreo del proceso**

  - ME1.1 Enfoque del monitoreo
  - ME1.2 Definición y recolección de datos de monitoreo
  - ME1.3 Método de monitoreo
  - ME1.4 Evaluación del desempeño
  - ME1.5 Reportes al consejo directivo y a ejecutivos
  - ME1.6 Acciones correctivas

Objetivo: Asegurar el logro de los objetivos establecidos para los procesos de TI. Lo cual se logra definiendo por parte de la gerencia reportes e indicadores de desempeño gerenciales y la implementación de sistemas de soporte así como la atención regular a los reportes emitidos.

Para ello la gerencia podrá definir indicadores claves de desempeño y/o factores críticos de éxito y compararlos con los niveles objetivos propuestos para evaluar el desempeño de los procesos de la organización. La gerencia deberá también medir el grado de satisfacción de los clientes con respecto a los servicios de información proporcionados para identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento, confeccionando informes que indiquen el avance de la organización hacia los objetivos propuestos.

- **M2 Evaluar lo adecuado del control interno**

  - ME2.1 Monitoreo del marco de trabajo de control interno
  - ME2.2 Revisiones de auditoría
  - ME2.3 Excepciones de control
  - ME2.4 Auto evaluación del control
  - ME2.5 Aseguramiento del control interno
  - ME2.6 Control Interno para terceros
  - ME2.7 Acciones correctivas

Objetivo: Asegurar el logro de los objetivos de control interno establecidos para los procesos de TI.

Para ello la gerencia es la encargada de monitorear la efectividad de los controles internos a través de actividades administrativas y de supervisión, comparaciones,

reconciliaciones y otras acciones rutinarias, evaluar su efectividad y emitir reportes sobre ellos en forma regular. Estas actividades de monitoreo continuo por parte de la Gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

- **M3 Obtención de aseguramiento independiente**

  - ME3.1 Identificar los requerimientos de las leyes, regulaciones y cumplimientos contractuales
  - ME3.2 Optimizar la respuesta a requerimientos externos
  - ME3.3 Evaluación del cumplimiento con requerimientos externos
  - ME3.4 Aseguramiento positivo del cumplimiento
  - ME3.5 Reportes integrados

Objetivo: Incrementar los niveles de confianza entre la organización, clientes y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo.

Para ello la gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos, como así también para trabajar con nuevos proveedores de servicios de tecnología de información. Luego la gerencia deberá adoptar como trabajo rutinario tanto hacer evaluaciones periódicas sobre la efectividad de los servicios de tecnología de información y de los proveedores de estos servicios como así también asegurarse el cumplimiento de los compromisos contractuales de los servicios de tecnología de información y de los proveedores de estos servicios.

- **M4 Proveer Auditoria independiente**

  - ME4.1 Establecimiento de un marco de gobierno de TI
  - ME4.2 Alineamiento estratégico
  - ME4.3 Entrega de valor
  - ME4.4 Administración de recursos
  - ME4.5 Administración de riesgos
  - ME4.6 Medición del desempeño
  - ME4.7 Aseguramiento independiente

Objetivo: Incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de auditorías independientes desarrolladas a intervalos regulares de tiempo. Para ello la gerencia deberá establecer los estatutos para la función de auditoría, destacando en este documento la responsabilidad, autoridad y obligaciones de la auditoria. El auditor deberá ser independiente del auditado, esto significa que los

auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado y en lo posible deberá ser independiente de la propia empresa.
Esta auditoría deberá respetar la ética y los estándares profesionales, seleccionando para ello auditores que sean técnicamente competentes, es decir que cuenten con habilidades y conocimientos que aseguren tareas efectivas y eficientes de auditoría.

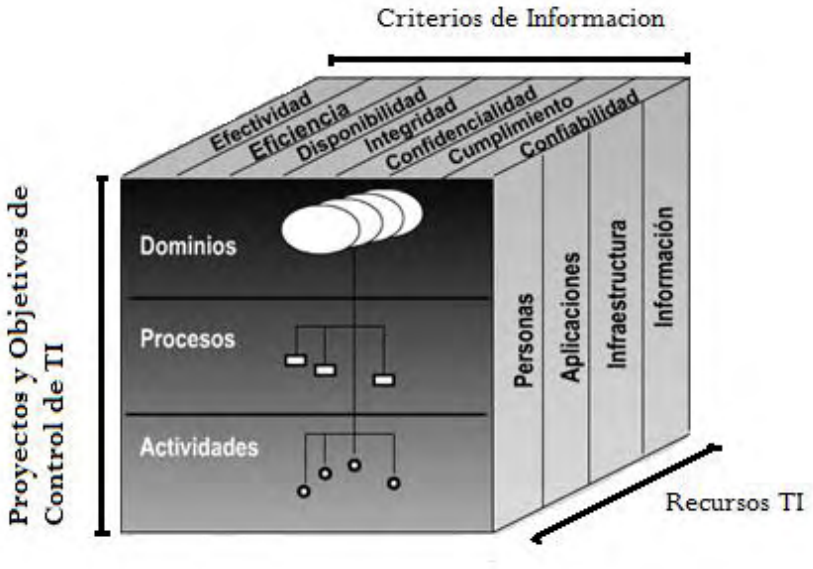
Un Control se define como "las normas, estándares, procedimientos, usos y costumbres y las estructuras organizativas, diseñadas para proporcionar garantía razonable de que los objetivos empresariales se alcanzaran y que los eventos no deseados se preverán o se detectaran, y corregirán"

Un Objetivo de Control se define como "la declaración del resultado deseado o propuesto que se ha de alcanzar mediante la aplicación de procedimientos de control en cualquier actividad de TI".

En resumen, la estructura conceptual se puede enfocar desde tres puntos de vista:

- Los recursos de las TI
- Los criterios empresariales que deben satisfacer la información
- Los procesos de TI

Figura 1: Las tres dimensiones conceptuales de COBIT



Las tres dimensiones conceptuales de COBIT

Estos dominios facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

Además, se toma en cuenta los recursos que proporciona la tecnología de información, tales como: datos, aplicaciones, plataformas tecnológicas, instalaciones y recurso humano.

Toda organización, necesita desarrollar una tecnología que le permita rediseñar actividades y procesos para lograr un mejor desempeño en las mismas, es así como el COBIT es fundamental en toda empresa, pues esta metodología reduce posibles vulnerabilidades y riesgos de los recursos de las tecnologías de información y así mismo evalúa el resultado de los objetivos de la empresa.

2.6 TÉCNICAS DE AUDITORIA DE SISTEMAS

2.6.1 Selección de áreas de auditoria. Dada la magnitud del universo por auditar, la revisión debe hacerse de manera selectiva, esta técnica es adecuada para empresas con múltiples localizaciones o sucursales, con el fin de dar prioridad a los procesos, se aplican evaluaciones estadísticas a estos en forma periódica, para poder clasificar cuales de estos procesos son claves para el proceso de auditoría.

2.6.2 Sistema de puntajes (Scoring). A diferencia de las anteriores técnicas la evaluación a los procesos y aplicaciones computarizadas se realiza de forma manual, con el fin de priorizar procesos con base en el análisis de riesgos, con la asignación de valores numéricos a las características claves, el auditor asignara la ponderación que este considere para cada factor, teniendo en cuenta el análisis de riesgo realizado con anterioridad que permita obtener un alto grado de confiabilidad , para llevar a cabo esta técnica se deberá diligenciar un formato de puntajes el que dará por resultado la clasificación para la auditoria.

2.6.3 Técnicas para operacionalizar la función de auditoría:

- **Software de auditoria multisitio.** Es una técnica aplicable a grandes empresas que tengan diferentes centros electrónicos de datos (PED, Procesamiento electrónico de datos). Desarrollando un programa o grupo de programas e instalándolos en las regionales para que sean utilizados por los auditores. Se requiere que se guarde uniformidad en el software utilizado en los PED para facilitar el proceso de auditotia, esta técnica es aplicada en ambientes de procesamiento distribuido.

- **Centros de competencia.** Esta técnica funciona a la inversa que la técnica de multisitio, ya que centra toda la información de las regionales en un centro de competencia y después de su análisis, evaluación e informes son enviados a las sucursales para tomar las respectivas decisiones.

2.6.4 Técnicas para examinar programas aplicativos:

- **Snapshot: Auditoría operativa y de sistemas de Información, herramientas de diagnóstico en tiempo record. (Imagen Instantánea).** Es una técnica que permite tomar una copia o una fotografía de la memoria de un proceso para llegar a la toma de decisiones en el momento de su actividad. Esta técnica tiene en cuenta los datos de entrada.

- **Mapping.** Es una técnica que utiliza una herramienta la cual permite evaluar cada una de las instrucciones de un programa, presentando reportes, tanto del número de veces que es ejecutada una instrucción como el tiempo que duró el procesador en ejecutarlas.

- **Tracing y flujograma de control.** El Tracing es una técnica muy importante en cuanto a los lenguajes de programación, puesto que identifica y muestra las instrucciones que fueron ejecutadas y en que secuencia aparecen.

3. METODOLOGÍA

Es necesario contar con una metodología para llevar un orden en la auditoria de sistemas de la Cooperativa del Magisterio de Túquerres – Coacremat, esta metodología es de tipo investigativa, cuantitativa y subjetiva, servirá como apoyo a la toma de decisiones, con unos objetivos que deberán ser cumplidos a cabalidad para lograr satisfacer el proceso de la auditoria donde se reunirá evidencia por parte del auditor para posterior mente analizarla y sacar unas conclusiones para fortalecer el sistema de información.

Con lo anterior, se plantea que la auditoria donde se comenzó a recolectar evidencias para hacer pruebas que proporcionaran unos datos para su posterior análisis, para la recolección de información se utilizó cuestionarios cuantificables con los funcionarios de los diferentes departamentos para hacer la pertinente toma de decisiones.

La metodología aplicada en la realización de esta auditoría, se hace de la siguiente manera:

Etapa I. Exploración y familiarización con el entorno.

En esta etapa se realiza una verificación de la empresa, conociendo sus diferentes procesos familiarizándose con las instalaciones de la empresa auditada. Esta exploración le permite al auditor analizar los objetivos a los que se debe llegar, también se realizaron visitas a los diferentes departamentos donde se utiliza el sistema de información mirando el manejo de los usuarios para lograr una mejor percepción de la información.

Una vez familiarizado con la empresa a ser auditada explorando sus diferentes procesos se procedió a realizar la auditoria de sistemas que pérmica conocer la vulnerabilidades de la empresa como también sus posibles soluciones.

Etapa II. Planeación de la auditoría de sistemas.

En esta etapa se realizó la planificación de la auditoria

- Identificar el alcance y los objetivos de la auditoria a realizar.
- Realizar el estudio inicial en la Cooperativa Del Magisterio De Túquerres COACREMAT, para recolectar datos sobre el funcionamiento del sistema.
- Determinar los recursos necesarios para realizar la auditoria.

- Elaboración del plan de trabajo

Etapa III. Realización de las actividades de la auditoría.

En esta etapa del proyecto se efectivizan las actividades planificadas en la fase anterior, aplicando distintas técnicas y utilizando herramientas que garanticen el cumplimiento de los objetivos planteados. Se realizan las siguientes actividades:

- Elaboración del plan de auditoría, a través de COBIT permitiendo así la identificación de los procesos y objetivos de control a evaluar.
- Realizar pruebas a los dominios y procesos seleccionados
- Elaborar Cuadros de Definición de Fuentes de Conocimiento de los procesos seleccionados
- Elaboración de cuestionarios cuantitativos para cada uno de los dominio seleccionados en cuanto al sistema de información
- Identificación de hallazgos.
- Asignación de la probabilidad de ocurrencia e impacto para los riesgos detectados mediante la aplicación del formato de hallazgos.
- Elaboración de la Matriz de Probabilidad e impacto, que permitió identificar los riesgos altos que necesitan mitigarse de manera urgente mediante un plan correctivo.

Etapa IV. Presentación del informe final.

En esta etapa del proceso de auditoría se presenta ante directivas de LA COOPERQTIVA DEL MAGISTERIO DE TUQUERRES COACREMAT, sustentando y presentando el informe donde se dan a conocer los problemas encontrados y se sugieren posibles soluciones.

4. DESARROLLO DEL TRABAJO

4.1 ARCHIVO PERMANENTE

Se incluye en este punto información permanente que sirve de consulta guía para la evaluación de políticas y procedimientos de la empresa, en este caso de la COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT.

4.1.1 Cooperativa del magisterio de Túquerres – Coacremat

4.1.1.1 Misión. Es una cooperativa multiactiva, presente en el Departamento de Nariño que presta servicios de asesoría, ahorro, crédito, comercialización y bienestar social para el mejoramiento de la calidad de vida de sus asociados; utilizando talento humano competente comprometido con la organización y con la tecnología adecuada.

4.1.1.2 Visión. Para el 2015 será reconocida como la primera opción de servicios solidarios y financieros para la comunidad educativa (docentes y administrativos), profesional e independiente en el sur occidente de Colombia.

4.1.1.3 Historia de la cooperativa del magisterio de Tuquerres. En una reunión de profesores la primera al comenzar el año escolar 1.976 -1977 el profesor LUIS ALVARO LEGARDA MERA propuso la creación de una cooperativa, igual a la que había organizado en un colegio de la Unión – Nariño y explicó algunas de las garantías que tenía formar estas entidades, entre ellas menciono créditos rápidos con fiadores entre los compañeros, bajos intereses menores a los de los bancos, requisitos mínimos, devolución de una parte de los intereses al final de año, adquisición de electrodomésticos y mercado para los socios.

La propuesta fue aceptada e inmediatamente inicio la participación de los asistentes definiendo que era más viable y menos riesgoso sometidos a votación 20 optaron por la cooperativa y 17 por el fondo. Democráticamente se continuo votando, luego por el monto de la cuota que inicio con el valor de $100 pesos para docentes y $50 pesos para administrativos, posteriormente definir a partir de qué fecha se inician los descuentos, determinando que desde el mes de septiembre y

solo dos docentes dijeron que a partir del mes de octubre, posteriormente se definió el valor de la cuota de afiliación en $30 pesos por socio[6].

Determinados todos los aspectos para comenzar a funcionar se nombró mediante el mismo proceso la junta directiva que fue conformada de la siguiente manera.

Gerente:	LUIS ALVARO LEGARDA MERA	EDGAR BACCA ARTEAGA
Tesorero:	JORGE EFRAIN FLOREZ MURIEL	JORGE VICENTE PAZ
Secretaria:	CIELO CENEIDA CALVACHE	LUCY MARIETA CAICEDO
Fiscal:	JOEL ADARVE MANRIQUE	LUIS MENESE SERAZA

A la mencionada junta se le encomendó hacer todos los contactos necesarios para realizar el curso de inducción cooperativa y así gestionar la personería jurídica. De esta manera entre el 25 y 28 de octubre la doctora LEONOR GARCIA DE PACHECO directora de la Superintendencia Nacional de Cooperativas y la doctora ANA LUCIA SALAZAR directora de la sección de educación de dicha superintendencia, capacitaron a todos los interesados en organizar la empresa que hoy se llama Coacremat.

Posterior a eso se obtuvo la personería jurídica #0452 del mes de mayo del año 1977 y el 14 de junio del mismo año se protocolizo la escritura #357 en la notaria primera del circuito de Túquerres.

Mediante resolución No. 0452 de Mayo 25 de 1.977 la COOPERATIVA DEL MAGISTERIO DE TUQUERRES LTDA.

Obtuvo de parte de la Superintendencia Nacional de Cooperativas, el reconocimiento legal mediante personería Jurídica y en Junio del mismo año, mediante escritura No. 357 de la Notaría primera de Túquerres se protocolizó la vida jurídica de la Cooperativa.

> Buscando brindar el mejor servicio, además de la ampliación y cobertura en el año 1977, se inició la apertura de la primera oficina en el Municipio de Samaniego, con los docentes del Colegio Simón Bolívar, este hecho dejó buenos resultados para la Cooperativa y es así como en el año 1991 se abrió la oficina en Pasto y año tras año se han abierto oficinas en varios municipios entre los cuales están: Túquerres, Ipiales, La Unión, Tumaco y Barbacoas. Dentro del ranking de las cooperativas de la misma naturaleza ocupamos el puesto Nº1 en el departamento de Nariño y el N°13 a nivel nacional.[7]

[6] http://www.coacremat.coop/coacremat/index.html

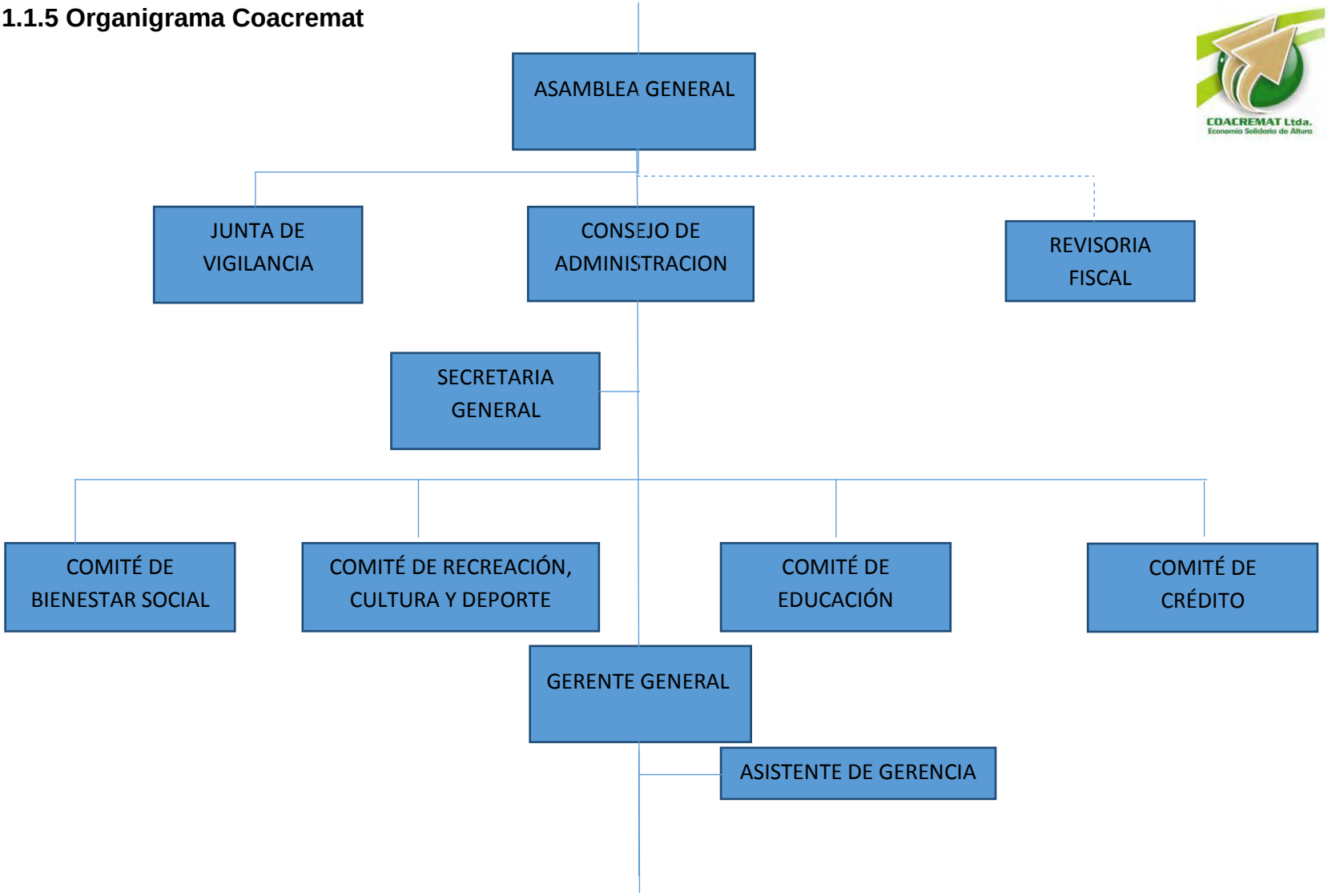
[7] Ibíd.

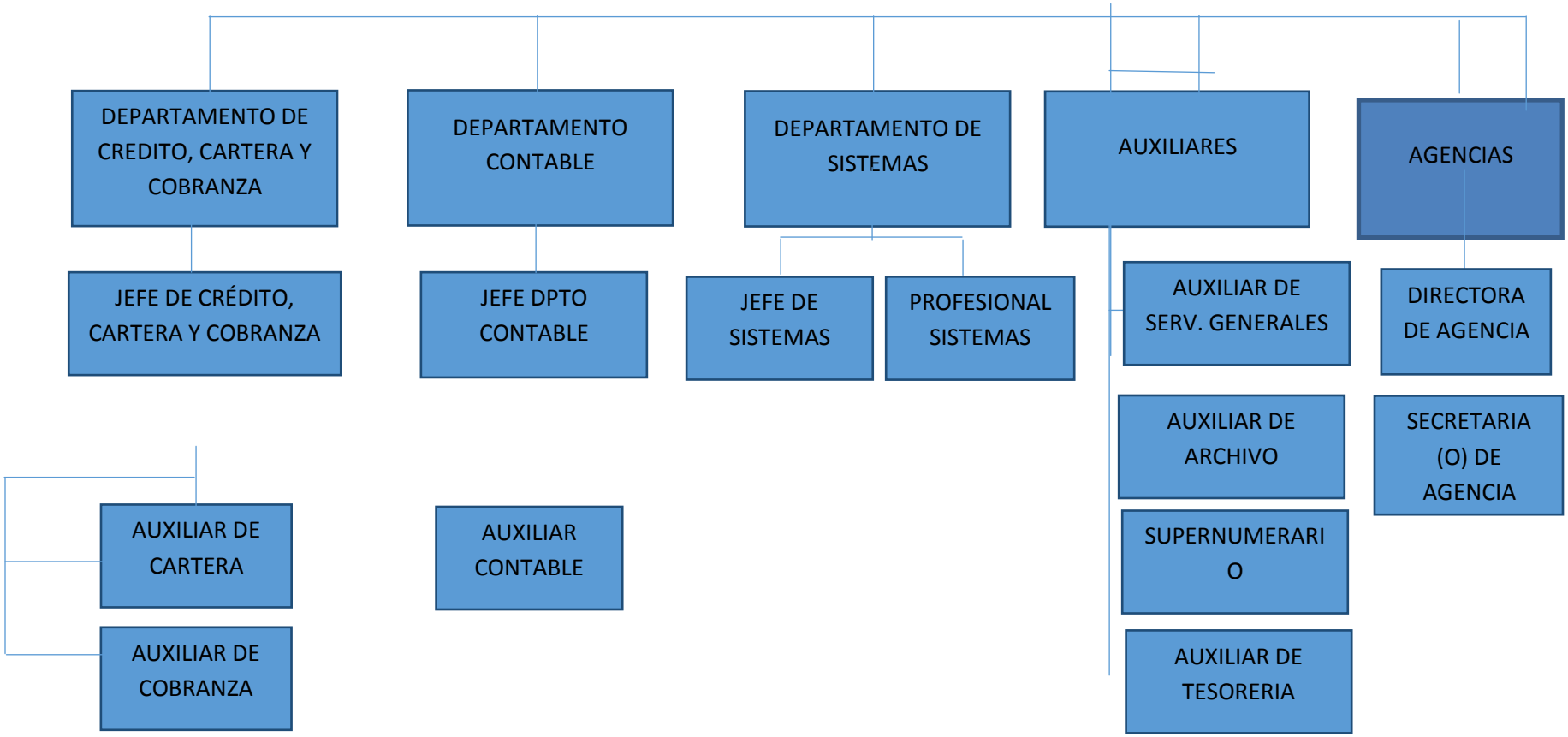
4.1.1.4 Departamento de sistemas. El departamento de sistemas de la Cooperativa del Magisterio de Túquerres Coacremat es un organismo que depende de la Gerencia Administrativa, encargado de la administración de los sistemas y soporte de los mismos, el objetivo de esta Área es la administración, organización y control de la información de Coacremat. Dentro de las actividades que se desarrollan en el departamento de sistemas corresponde a la administración del sistema linix con el objetivo de garantizar el manejo de la información y facilitar su utilización a todas las dependencias de la empresa en general. También se encarga de las funciones de Comunicaciones, la implementación y el mantenimiento de la plataforma tecnológica, la infraestructura informática de red de la empresa, configuraciones, investigación de nueva tecnología y diferentes procedimientos para el buen manejo de la información de Coacremat.

Dentro de las actividades que se desarrollan en el departamento de sistemas de Coacremat se tienen las siguientes:

- Mantenimiento de los equipos
- Gestión de cuentas de usuario
- Necesidades de recursos informáticos y desarrollo de software
- Preservación de la seguridad de los sistemas
- Privacidad de los datos de usuario, incluyendo copias de seguridad periódicas.
- Instalación, configuración y mantenimiento de servicios como correo electrónico, proxy Web, entre otros.
- Instalación y actualización de software.
- Instalación y configuración de la red de datos.
- Administración del Servicio de Web
- Seguridad en la red
- Mantenimiento de Servidores
- Instalación y actualización del software.
- Backups.
- Instalación y configuración de aplicaciones en los servidores.
- Elección de Sistemas Operativos.
- Administración de Sistemas
- Gestión y administración de bases de datos.
- Soporte de Aplicaciones
- Ofimática
- Asesoramiento y capacitación de usuarios.
- Elaboración de informes

4.1.1.5 Organigrama Coacremat




DEPARTAMENTO DE CREDITO, CARTERA Y COBRANZA
DEPARTAMENTO CONTABLE
DEPARTAMENTO DE SISTEMAS
AUXILIARES
AGENCIAS
JEFE DE CRÉDITO, CARTERA Y COBRANZA
JEFE DPTO CONTABLE
JEFE DE SISTEMAS
PROFESIONAL SISTEMAS
AUXILIAR DE SERV. GENERALES
DIRECTORA DE AGENCIA
AUXILIAR DE ARCHIVO
SECRETARIA (O) DE AGENCIA
AUXILIAR DE CARTERA
AUXILIAR CONTABLE
SUPERNUMERARIO
AUXILIAR DE COBRANZA
AUXILIAR DE TESORERIA

4.2 ARCHIVO CORRIENTE

Para hacer la auditoria es necesario acumular información que será utilizada por el auditor que tendrá que ver con el desarrollo de los diferentes dominios de COBIT.

4.2.1 Plan de auditoria

4.2.1.1 Objetivos:

Objetivo general: Realizar el estudio, revisión, verificación y evaluación del SISTEMA DE INFORMACIÓN DE LA COOPERATIVA DEL MAGISTERIO DE TUQUERRES – COACREMAT observando el cumplimiento de las diferentes normas mediante la auditoria a la seguridad física, seguridad lógica, infraestructura tecnología y software.

Objetivos específicos:

- Obtener una evaluación real y efectiva sobre los posibles riesgos delictivos presentes en sistema de información de Coacremat.
- Identificar y analizar las diferentes vulnerabilidades que se pueden presentar en cada una de los componentes del sistema de información.
- Verificar la aplicación de barreras y procedimientos que resguarden el acceso a los datos.
- Comprobar que tipo de mantenimiento reciben los equipos que conforman la plataforma tecnológica
- Comprobar las licencias de los programas instalados en los terminales de cada una de las áreas que conforman la Cooperativa del Magisterio de Túquerres en su sede principal.

4.2.1.4 Alcance. La auditoría pretende identificar las condiciones actuales del Sistema de información de la cooperativa del magisterio de Túquerres – Coacremat en los siguientes ítems:

Seguridad física: Se verificará las condiciones ambientales que permiten estar protegidos mediante elementos que combinados, ayudan a integrar una serie de medidas preventivo-disuasivas o represivas contra eventualidades de carácter ilícito.

Seguridad lógica: verificar los diferentes controles de acceso a la información, como también los diferentes roles que tienen los clientes internos para utilizar el sistema de información comprobando la limitación a los servicios que tienen dichos usuarios.

Infraestructura tecnológica: Se evaluará el tipo de mantenimiento que tienen cada uno de los terminales así como su hoja de vida, comprobando su respectivo uso de acuerdo al usuario.

Software: verificar las licencias de funcionamiento de los diferentes programas instalados en Coacremat. Lo anterior con el fin de observar un conjunto de elementos para verificar el cumplimiento de normas y así optimizar el uso de los recursos para brindar un buen servicio a los asociados de dicha empresa.

4.2.1.5 Justificación. Realizar una auditoría de sistemas al sistema de información de la Cooperativa del Magisterio de Túquerres Coacremat, evaluado cada uno de los ítems anteriormente nombrados para verificar, evaluar y analizar los diferentes hallazgos así como sus posibles soluciones para que se realicen mejoras, esto con el fin de mejorar en los diferentes aspectos para un buen funcionamiento y mejoramiento del servicio de sus asociados.

4.2.1.6 Metodología. Para el cumplimiento de los objetivos planteados en la auditoría, se realizaran las siguientes actividades:

- **Investigación preliminar:**

Determinar la estructura organizacional de la Cooperativa del magisterio de Túquerres Coacremat para determinar responsables en la vigilancia del sistema de información instalado.

Evaluar la importancia de la seguridad física, lógica, infraestructura tecnológica y software dan a los procesos de Coacremat.

Conocer de manera global el sistema de información instalado y configurado para el manejo de los servicios, identificando los elementos que apoyan la seguridad y administración de la misma.

- **Identificación y agrupación de riesgos:**

Identificar y clasificar los riesgos a los que está expuesto el sistema de información, ya sean propios o generados por entidades externas (personas, procedimientos, bases de datos, redes, virus etc.) esto se hace por medio de las

visitas que se realizan para la familiarización del auditor con el sistema de información

- **Diseño del programa de auditoría:**

Definir los dominios, procesos y objetivos de control de COBIT, que tienen relación con el proceso de auditoría.

Realizar los procedimientos que permitan recolectar la evidencia que apoye los hallazgos y recomendaciones.

- **Ejecución de las pruebas de auditoría:**

Obtener evidencia sobre los procesos establecidos, su utilización, y el entendimiento y ejecución de los mismos por parte de las personas involucradas.

Identificar las causas de las debilidades

Determinar la probabilidad y el impacto que tendrá cada debilidad en el sistema de información.

Identificar los hallazgos de tipo preventivo, defectivo y correctivo de las debilidades encontradas.

Identificar los recursos afectados por las debilidades encontradas

- **Elaboración y envío del informe de auditoría:**

Comunicar a las personas o entes involucrados en la vigilancia y administración del sistema de información de Coacremat, los resultados de la auditoria, para que ellos hagan la gestión necesaria para implementar los controles que cubran aquellas situaciones de riesgo de mayor relevancia, y mantengan y optimicen la red.

Hacer parte de la documentación para futuras auditorías.

4.2.1.7 Herramientas de estudio:

- ✓ Evidencia fotográfica.
- ✓ cuestionarios de Análisis de riesgo.
- ✓ Entrevistas.
- ✓ Inventarios equipos

4.2.1.8 Recursos

- Humanos:

José Alexander melo Ipújan, estudiante de Ingeniería de sistemas:

- Técnicos
- Computador.
- Impresora.
- Cámara Digital.
- Grabadora de voz

4.2.2. Programa de auditoria. Para la realización de la auditoria de sistema a la Cooperativa del Magisterio de Túquerres Coacremat, se utilizara la metodología COBIT (objetivos de control para la información y tecnologías relacionadas) donde existen 4 dominios de los cuales se evaluaran los siguientes:

4.2.1.1 Objetvos de control para la cooperativa del magisterio de Tuquerres:

DOMINIO DE PLANEACION Y ORGANIZACIÓN (PO)

Este dominio se relaciona con la identificación de la tecnología de información y comunicación en Coacremat, donde contribuye a los diferentes logros, metas y objetivos de la organización haciéndolo a través de un conocimiento TIC para lograr ejecutar una auditoria donde se evaluaran los siguientes procesos:

P02. Definir la arquitectura de la información

Se encarga de evaluar el modelo de datos en la infraestructura tecnológica de Coacremat, así como sus diferentes niveles de seguridad correspondientes a cada dato.

- **PO2.1 Modelo de arquitectura de información empresarial**: Proceso encargado de administrar y dirigir el modelo de información con los diferentes recursos de tecnología de información y comunicación en Coacremat.
- **PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos:** Debe existir un diccionario de datos para lograr mayor organización en cuanto a la información ya que este facilita una estructura de información y como compartir los datos en la empresa.

- **PO2.3 Esquema de clasificación de datos:** Es necesario mantener un esquema de clasificación de datos en Coacremat ya que esta permite clasificar la información con diferentes niveles de seguridad, permitiendo solo acceder a personal autorizado para la utilización de los diferentes archivos.

P03. Determinar la dirección tecnológica

Facilita la evaluación en los diferentes recursos tecnológicos de cooperativa ya que esta debe tener un plan de infraestructura tecnológica que sea utilizado para tener mejores servicios en cuanto a las TIC, identificando cada punto del plan de infraestructura tecnológica para mirar el potencial de la empresa desde el punto de vista tecnológico hacia un futuro.

- **PO3.1 Planeación de la dirección tecnológica:** De acuerdo a las capacidades de las empresa se tiene una tecnología en el sistemas de información con lo cual se debe tener una planeación para analizar estas tecnologías y que es lo más apropiado para la organización.

- **PO3.2 Plan de infraestructura tecnológica:** Es necesario que la empresa tenga un plan de infraestructura tecnológica ya que la empresa debe conocer sus objetivos en cuanto a las tecnologías y esto debe estar plasmado en unos planes para que sean evaluados para una posterior implementación de nuevos recursos tecnológicos.

- **PO3.3 Monitoreo de tendencias y regulaciones futuras:** Es necesario tener un monitoreo permanente en la empresa en la tecnología que esta tiene para poder resolver problemas antes de que estos se puedan dar haciendo más competitivo la parte del sistema de información.

- **PO3.4 Estándares tecnológicos:** Evaluar y verificar los estándares tecnológicos de la empresa tales como productos de la infraestructura y guías sobre la selección de la tecnología.

P04. Definir los procesos, organización y relaciones de TI

Entregar los servicios correctos de TI por parte de los funcionarios es importante realizar una organización adecuada en los roles, habilidades y responsabilidades, alineados con el negocio que facilita la estrategia y provee la orientación efectiva y el control adecuado a los diferente procesos.

- **PO4.5 Estructura organizacional:** En el área de sistemas de Coacremat es importante tener una estructura organizacional de cargos y responsabilidades ya que esta interactúa directamente con el sistema de información haciendo un equipo de trabajo para realizar los procesos de forma óptima.

- **PO4.6 Establecimiento de roles y responsabilidades:** Se debe tener en la empresa el personal pertinente con el perfil adecuado para realizar las diferentes tareas que se les asigna, teniendo en cuenta los roles que el personal debe desempeñar con sus responsabilidades establecidas para que las funciones y tareas interactúen con el sistema de información de manera adecuada.

- **PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento:** El área de sistemas deberá tener en cuenta el riesgo permanente en la empresa para que los profesionales en sistemas estén preparados para adoptar medidas de contingencia para proteger el sistema de información.

- **PO4.9 Propiedad de datos y de sistemas:** Se debe identificar y supervisar la integridad de los datos para que no sean cambiados, controlando así la información que es transmitida por diferentes medios de comunicación.

- **PO4.10 Supervisión:** Es necesario la supervisión del sistema de información con todos sus componentes, así como su entrada procesamiento de datos y salida de información.

P07. Administrar los recursos humanos de TI

En la cooperativa del magisterio de Túquerres se debe tener el personal idóneo, entrenado y capacitado para interactuar con las diferentes tecnologías que se tienen hoy en día, es así que el personal debe estar en constante capacitación para lograr un mejor rendimiento en la empresa utilizando las herramientas tecnológicas para mejorar la producción de la información.

- **PO7.1 Reclutamiento y retención del personal:** Se debe tener unas buenas prácticas de contratación para el reclutamiento y promoción del personal.

- **PO7.2 Competencias del personal:** Se debe hacer un monitoreo constante con el personal que accede al sistema de información de la cooperativa para ver la aplicación de las buenas prácticas de TIC dentro de la empresa con un perfil adecuado en cuanto a su rol y trabajo.

- **PO7.3 Asignación de roles:** Planear una revisión de los roles del personal para comprobar los requerimientos que la empresa necesita para hacerlos participes de diferentes capacitaciones en cuanto a ellas.

- **PO7.4 Entrenamiento del personal de TI:** El personal de Coacremat debe estar en constante capacitación ya que los sistemas de información están en continuo cambio por eso es importante las capacitaciones para generar confianza en el manejo del sistema.

P09. Evaluar y administrar los riesgos de TI

Se debe tener planes de contingencia para disminuir el riesgo de la posibilidad de ocurrencia de siniestro de hardware o de software.

- **PO9.1 Marco de trabajo de administración de riesgos:** Hacer una evaluación de riesgos que la Cooperativa del Magisterio de Túquerres puede tener a largo plazo, identificando los riesgos y sus posibles soluciones.

- **PO9.2 Establecimiento del contexto del riesgo:** El sistema de información de Coacremat como una fuente vital de información y se debe tener una administración de riesgos con diferentes criterios para así tener un plan de contingencia que se active cuando suceda un siniestro en el sistema.

- **PO9.3 Identificación de eventos:** Se deben realizar monitoreos y autoevaluaciones constantes al sistema de información para identificar posibles vulnerabilidades clasificarlas y ver en que afectan si se dejan sin un control adecuado para detenerlas.

- **PO9.4 Evaluación de riesgos de TI:** Los riesgos evaluados deben ser calificados para ver la probabilidad de impacto que generan dentro del sistema de información usando métodos cualitativos y cuantitativos.

- **PO9.5 Respuesta a los riesgos:** Se debe tener un plan de acción para minimizar la probabilidad de evento e impacto de los riesgos minimizando su capacidad de daño en el sistema de información.

- **PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos:** Es necesario establecer un plan de acción de riesgos donde se identifiquen cada uno de los riesgos y amenazas con un plan de acción donde se encuentren las posibles soluciones.

DOMINIO DE ADQUISICION E IMPLEMENTACION (AI)

El software es un activo importante en la Coacremat y este hace que los procesos sean más fáciles de manejar pero para esto se debe implementar aplicativos que en realidad le sirvan a la cooperativa teniendo en cuenta tres aspectos importantes como los son la necesidad el análisis y la compra.

AI2 Adquirir y mantener software aplicativo: Los aplicativos de la empresa deben ser necesarios y se deben obtener después de hacer un análisis del problema para mejorar el sistema de información.

- **AI2.1 Diseño de alto nivel:** Es necesario evaluar, analizar lo requerimientos de la empresa para realizar desarrollos de aplicativos dentro del sistema de

información que fortalezcan los procesos que se desarrollan dentro de Coacremat.

- **AI2.2 Diseño detallado:** Se debe desarrollar aplicativos que sean seguros para la empresa y se sustenten como un camino para esquivar problemas dentro del sistema de información.

- **AI2.3 Control y posibilidad de auditar las aplicaciones:** Para una mejor protección del sistema en la empresa se debe tener un plan donde se auditen las aplicaciones teniendo en cuenta el rendimiento, nivel de operatividad y uso.

- **AI2.4 Seguridad y disponibilidad de las aplicaciones:** Se deben realizar monitoreos y autoevaluación a las aplicaciones que se desarrollen en la empresa para ver cómo se comportan con la información que tiene el sistema.

- **AI2.5 Configuración e implantación de software aplicativo adquirido:** Se debe realizar un plan de configuración e implantación de los aplicativos, así como unos periodos de prueba para mirar su eficacia.

- **AI2.6 Actualizaciones importantes en sistemas existentes:** El sistema linix que es uno de los ejes fundamentales de todo el sistema de información debe ser modular, ósea que se pueda implementar otros programas para generar más información según los requerimientos de Coacremat.

- **AI2.7 Desarrollo de software aplicativo:** El desarrollo de aplicativos se deben realizar de acuerdo a los estándares siguiendo unas normas y un proceso para generar una automatización de procesos con dicho software.

- **AI2.8 Aseguramiento de la calidad del software:** Se debe realizar un proceso para el desarrollo de aplicaciones analizando los requerimientos del problema y la solución tecnológica a este, para mejorar la calidad de la información y del sistema, todo el proceso debe estar documentado para posteriores consultas.

- **AI2.9 Administración de los requerimientos de aplicaciones:** ES importante documentar todo el proceso del desarrollo de la aplicación y de los requerimientos durante el proceso de diseño y codificación.

- **AI2.10 Mantenimiento de software aplicativo:** Es imprescindible que se haga mantenimiento a las aplicaciones por parte de Coacremat y del sistema linix por parte de los desarrolladores.

AI3 Adquirir y mantener infraestructura tecnológica

Se debe garantizar una infraestructura tecnológica que satisfaga las necesidades de la empresa teniendo en cuenta el presupuesto y los procesos que se vayan a automatizar.

- **AI3.1 Plan de adquisición de infraestructura tecnológica:** Se debe tener un plan que defina las diferentes adquisiciones que hace la empresa en cuanto a la tecnología de plataforma tecnológica en Coacremat.

- **AI3.2 Protección y disponibilidad del recurso de infraestructura:** Es importante tener un plan de configuración y de protección para la infraestructura tecnológica de la empresa donde se garantice la disponibilidad de los diferentes dispositivos que componen la plataforma tecnológica.

- **AI3.3 Mantenimiento de la infraestructura:** Es necesario tener un plan de mantenimiento de la plataforma tecnológica y de la red de datos**,** donde se realicen diferentes actividades como una autoevaluación y monitoreos a estos dispositivos.

- **AI3.4 Ambiente de prueba de factibilidad:** Evaluarlos diferentes ambientes donde se pueda soportar la eficiencia y eficacia de la plataforma tecnología y la red de datos.

AI5 Adquirir recursos de TI

Establecer los estándares a nivel interno de la organización para la adquisición de TI, instalaciones, hardware y software.

- **AI5.1 Control de adquisición:** Se tiene que hacer un análisis de los recursos que se van a adquirir ya sea hardware o software para la organización, donde se evaluara este procedimiento mirando las instalaciones físicas y de la plataforma tecnología.

- **AI5.2 Administración de contratos con proveedores:** Revisar los diferentes contratos que se han realizado con los proveedores teniendo en cuenta políticas internas de la empresa.

- **AI5.3 selección de proveedores:** Para desarrollar una buena política de compras es necesario que los proveedores se ajusten a la empresa para adquirir un producto, es importante evaluar los factores de calidad de los proveedores.

- **Al5.4 Adquisición de recursos TI:** Se tiene que realizar contratos que le convenga a la empresa donde el proveedor se comprometa a cumplirá con todo lo que dice antes de hacer la compra, respetando el contrato de los productos tecnológicos comprados.

Al6 Administrar cambios:

Los cambios que se realizan en el sistema de información deben seguir unos estándares y procedimientos que identifique y garantice una solicitud de cambio evaluada de manera correcta y estructurada. Los cambios que Coacremat ha implantado en su sistema de información deben surgir de la necesidad y de actualización de dispositivos ya que la tecnología y los sistemas van cambiando a través del tiempo.

- **Al6.1 Estándares y procedimientos para cambios:** Se deben solicitar cambios de forma oportuna para hacer la respectiva evaluación y análisis de los mismos donde la gerencia debe apoyar estas medidas según le convenga a la empresa.

- **Al6.2 Evaluación de impacto priorización y recuperación:** Las diferentes solicitudes de cambio se deben generar a través de una evaluación de prioridades que requiere el sistema de información analizando el impacto donde se establezca que pasaría si no se hace dicho cambio y que beneficios traería al sistema de información.

- **AL6.3 Cambios de emergencia:** Se debe establecer una guía para establecer un proceso rápido y eficaz que logre satisfacer el cambio de manera inmediata para no estropear el normal transcurso del sistema de información.

- **Al6.4 Seguimiento y reporte del estatus de cambio:** Evaluar si existen reportes de cambio de infraestructura en Coacremat, este debe estar con su debido proceso de análisis del problema y ejecución de cambio.

- **Al6.5Cierre y documentación del cambio:** Todo cambio al sistema de información debe estar documentado para garantizar las compras que se han realizado.

DOMINIO DE ENTREGAR Y DAR SOPORTE

El soporte en una empresa es uno de los factores más importantes ya que a través de este se pueden realizar capacitaciones a los usuarios que utilizan los

sistemas de información, además que las empresas contratistas están obligadas a hacer este tipo de soportes para la empresa.

DS3 Administrar el desempeño y la capacidad

Asegurar que la capacidad y desempeño adecuado esté disponible y que se haga el mejor y el óptimo uso del sistema para satisfacer las necesidades requeridas de la empresa.

- **DS3.1 Planeación del desempeño y la capacidad:** Evaluar el proceso de planeación para mirar el desempeño del sistema de información tanto como en su hardware como en su software.

- **DS3.2 Capacidad y desempeño actual:** Evaluar el desempeño actual del sistema, verificando la autoevaluación que le hacen los encargados de administrar el sistema de información.

- **DS3.3 Capacidad y desempeño futuros:** La autoevaluación en el desempeño del sistema en general es importante porque este mide la capacidad de distribución de datos a través de la red, mirando la capacidad de procesamiento con la plataforma tecnológica.

- **DS3.4 Disponibilidad de recursos de TI:** Evaluar cómo responde el sistema a las diferentes cargas de trabajo y si mirar la disponibilidad cuando se satura o cuando ocurre un siniestro simple como el fluido de energía.

- **DS3.5 Monitoreo y reporte monitorear:** Determinar el pronóstico de las diferentes monitoreos y autoevaluaciones del sistema en su plataforma tecnológica y su red de datos.

DS4 Garantizar la continuidad del servicio

Se debe tener un plan de contingencia para que se garantice el normal funcionamiento de los servicios tecnológicos.

- **DS4.1 Marco de trabajo de continuidad de TI:** Coacremat como empresa solidaria donde se registran muchos procesos al día debe tener una metodología para que la continuidad de los procesos se garanticen en este caso el del servidor y toda la plataforma tecnológica.

- **DS4.2 Planes de continuidad de TI:** Evaluar los planes de contingencia que se tengan y como se desarrollan ante una eventual catástrofe.

- **DS4.3 Recursos críticos de TI:** Establecer los puntos críticos en la infraestructura tecnológica estos deben estar en los planes de contingencia y se deben dar prioridad según la necesidad de los procesos y de los usuarios como por ejemplo el servidor de Coacremat ya que este contiene toda la información de la empresa y de los usuarios.

- **DS4.4 Mantenimiento del plan de continuidad de TI:** los planes de continuidad tienen que estar en constante actualización y vigente para servicios que se hayan implantado recientemente en la empresa.

- **DS4.5 Pruebas del plan de continuidad de TI:** Si la empresa cuenta con un plan de continuidad este se debe someter a pruebas continuas para observar el comportamiento y si es necesario su actualización.

- **DS4.6 Entrenamiento del plan de continuidad de TI: En** el plan de continuidad debe participar todas las personas involucradas según su función y se las debe capacitar y darles a conocer cuando se active el plan de continuidad.

- **DS4.7 Distribución del plan de continuidad de TI:** Se debe establecer una adecuada distribución del plan de contingencia para que los usuarios conozcan lo que contiene dicho plan y qué hacer cuando este activado.

- **DS4.8 Recuperación y reanudación de los servicios de TI:** Proceso de restaurar las operaciones luego de un mal funcionamiento o de alguna catástrofe, así se asegurara la disponibilidad de la información.

- **DS4.9 Almacenamiento de respaldos fuera de las instalaciones:** Es importante para cualquier entidad proteger su información y sacarle una copia de seguridad a los datos. Por eso es imprescindible en empresas que manejan dinero hacerlo y tener un servidor espejo que contengan toda la información.

DS5 Garantizar la seguridad de los sistemas

Salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida. Para ello se realizan controles de acceso lógico que aseguren que el acceso al sistema, datos y programas esté restringido a usuarios autorizados.

- **DS5.1 Administración de la seguridad de TI:** Evaluar cómo se administra la seguridad del sistema de información.

- **DS5.2 Plan de seguridad de TI:** Debe existir un plan de seguridad donde se muestren las debilidades y fortalezas de cada uno de los elementos del sistema de información y como mitigar sus efectos.

- **DS5.3 Administración de identidad:** Las personas que entran a la cooperativa deben ser identificados, así como los usuarios del sistema que deben tener un permiso para acceder al sistema de Coacremat.

- **DS5.4 Administración de cuentas del usuario:** Todo usuario debe tener una cuenta con su clave de acceso para que esta le permita ver lo que realmente le concierne dependiendo de su función.

- **DS5.5 Pruebas, vigilancia y monitoreo de la seguridad:** Evaluar si se hacen pruebas de seguridad al sistema de información y a la red de datos, estos son importantes para el sistema y si alguien llega a entrar a esta red puede capturar los datos copiarlos o dañarlos.

- **DS5.6 Definición de incidente de seguridad:** Es necesario tener un archivo de incidencias de seguridad ya que estas servirían para poder encontrar otras a futuro y podrían aplicarse para mejorar la seguridad dentro del sistema de información.

- **DS5.7 Protección de la tecnología de seguridad:** El sistema debe estar preparado para cualquier clase de sabotaje es por eso que las copias de seguridad son importantes para proteger la integridad de los datos.

- **DS5.9 Prevención, detección y corrección de software malicioso:** Es necesario contar con un software especializado y licenciado, que realice las tareas de detección y corrección de software.

- **DS5.10 Seguridad de la red:** Es importante proteger la red de datos de cualquier tipo de intervención de elementos externos. Debe contar con claves de seguridad y con un escaneo donde se muestre los usuarios que están utilizando la red.

DS8 Administrar la mesa de servicio y los incidentes

A los asociados de la Cooperativa del Magisterio de Túquerres – Coacremat se les debe responder de manera oportuna las consultas y los problemas que ocurran durante el periodo de afiliación.

- **DS8.1 Mesa de servicios:** Establecer si la cooperativa del magisterio de Túquerres tiene diseñada una mesa de servicios y si realiza una correcta ejecución de esta.

DS9 Administrar la configuración

Su objetivo es llevar un registro actualizado de todos los elementos de configuración de la infraestructura del sistema de información, por lo tanto es esencial conocer la infraestructura de Coacremat para obtener el mayor provecho de la misma.

- **DS9.1 Repositorio y línea base de configuración:** Evaluar si existe una herramienta o procedimiento para realizar las configuraciones de la plataforma tecnológica donde se mire las características de configuración de las maquinas.

- **DS9.2 Identificación y mantenimiento de elementos de configuración:** Establecer una autoevaluación al proceso o plan de mantenimiento donde se debe encontrar las características del mantenimiento y la configuración del hardware.

- **DS9.3 Revisión de integridad de la configuración:** Evaluar si existe un procedimiento donde se observe como se dejó el dispositivo después de su configuración y como se lo encuentra después de un determinado tiempo.

DS10 Administración de problemas

El proceso de administración de problemas se hace a todos los niveles de la Coacremat. Las responsabilidades y la propiedad de los problemas deben estar claramente establecidas. Los procedimientos son documentados, comunicados y medidos para evaluar su efectividad. La mayoría de los problemas deben estar identificados, registrados y reportados, con su respectiva solución.

- **DS10.1 Identificación y clasificación de problemas: La** existencia de un repositorio donde se reporten los problemas de la Coacremat es importante porque a través de esta podemos tener un historial y una solución a problemas que hayan sucedido anteriormente y que se pueden dar en el futuro.

- **DS10.2 Rastreo y resolución de problemas:** Con la existencia de un repositorio se puede hacer la clasificación de problemas con sus posibles soluciones.

- **DS10.3 Cierre de problemas:** Evaluar la solución de los problemas y si existe un proceso de cierre y verificación de la solución del problema.

DS11 Administración de datos

Se debe garantizar la integridad de los datos, que estos no sean modificados, que lleguen a su destino sin ninguna alteración y no sean repetidos, para que estén disponibles cuando el personal con acceso a los datos lo requieran.

- **DS11.1 Requerimientos del negocio para administración de datos:** Los datos procesados en la Coacremat deben estar disponibles cada vez que se requieran guardando su integridad.

- **DS11.2 Acuerdos de almacenamiento y conservación:** Verificar el estado de las copias de seguridad, si estas están en medio magnético, digital y en un lugar adecuado.

- **DS11.4 Eliminación:** La eliminación de datos debe ser segura desde cualquier computadora contando siempre con una copia de seguridad.

- **DS11.5 Respaldo y restauración:** Verificar la capacidad de reacción frente a un incidente informático en cuanto a acceder a los datos de forma rápida utilizando las copias de seguridad y que proceso siguen para su restauración inmediata.

DS12 Administración del ambiente físico

La importancia del ambiente físico para un sistema de información como el de Coacremat debe ser un lugar adecuado para que el sistema funcione de manera efectiva y debe estar protegido contra peligros naturales o fallas humanas.

- **DS12.1 Selección y diseño del centro de datos:** Se debe reunir con los requerimientos que un centro de datos lo requiere en este caso los servidores de la Cooperativa del Magisterio de Túquerres.

- **DS12.2 Medidas de seguridad física:** Se debe tener medidas de seguridad para la plataforma tecnológica del sistema, así como en su red de datos ya que puede suceder un acontecimiento en cualquier momento.

- **DS12.3 Acceso Físico:** La seguridad empresarial es importante y el acceso a los diferentes recursos tecnológicos debe ser restringido y seguro.

- **DS12.4 Protección contra factores ambientales:** Es importante que se adopten planes de contingencia para la protección de datos y del sistema de información para minimizar los daños.

- **DS12.5 Administración de instalaciones físicas:** Se deben seguir los lineamientos para la implantación de sistemas de información tanto en redes de datos, servidores, routers y plataforma tecnológica.

Dominio: Monitorear y evaluar (ME)

Es importante monitorear los procesos de Coacremat dentro de su sistema de información para luego evaluar y analizar los resultados donde se pueden sacar varias conclusiones.

ME1 Monitorear y evaluar el desempeño de TI

El desempeño de los diferentes dispositivos que conforman el sistema de información de Coacremat es fundamental ya que muestra indicadores sobre el funcionamiento y se pueden establecer medidas si está en un mal funcionamiento.

- **ME1.1 Enfoque del monitoreo:** El monitoreo de procesos en el sistema se tiene que hacer constantemente porque se avaluara el desempeño de este.

- **ME1.2 Definición y recolección de datos de monitoreo:** Evaluar si la corrección de datos del monitoreo se implementa para realizar el mantenimiento necesario dentro del sistema de información.

- **ME1.3 Método de monitoreo:** Verificar si existe un método de monitoreo eficaz para hacer la recolección de datos adecuada.

- **ME1.4 Evaluación del desempeño:** Con los monitoreos realizados compararlos con los objetivos que la empresa realiza con la ayuda del sistema, así analizando los resultados para dar unas conclusiones.

- **ME1.5 Reportes al consejo directivo y a ejecutivos:** Verificar si existen reportes de los análisis de monitoreo del sistema.

- **ME1.6 Acciones correctivas:** Hacer las diferentes correcciones basadas en el monitoreo y como se implementarían en el sistema de información.

4.2.2 Diseño de elementos de la auditoria: Para la realización del proceso de auditoría a la Cooperativa del Magisterio de Túquerres - Coacremat, se utilizaron diferentes instrumentos de recolección de información, a continuación se describe cada uno de ellos:

Cuadro de definición de fuentes de conocimiento, pruebas de análisis, y pruebas de auditoría: Este cuadro es un instrumento que sirve para identificar, cuál es la información que se necesita para evaluar un determinado proceso dentro de los dominios del COBIT, también se especifica en el cuales son las pruebas de análisis y de ejecución que se deben realizar. Los ítems relacionados a continuación son los que describirán el elemento de auditoría.

- ✓ **REF:** Se refiere al ID del elemento.

- ✓ **ENTIDAD AUDITADA:** En este espacio se indicara el nombre de la entidad a la cual se le está realizando el proceso de auditoría.

- ✓ **PROCESO AUDITADO:** En este espacio se indicara el nombre del proceso objeto de la auditoria, para el caso será Contratación TI.

- ✓ **RESPONSABLES:** En este espacio se indicaran los nombres del equipo auditor que está llevando a cabo el proceso de auditoría.

- ✓ **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA:** En este espacio se hace una breve referencia al objetivo del proceso seleccionado dentro de los dominios del COBIT que se está revisando.

- ✓ **MATERIAL DE SOPORTE:** En este espacio se indicara el nombre del material que soporta el proceso, para el caso será COBIT.

- ✓ **DOMINIO:** Espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.

- ✓ **PROCESO:** Espacio reservado para el nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.

- ✓ **FUENTES DE CONOCIMIENTO:** En este espacio se deberá consignar todas las fuentes de donde se extrajo la información para el proceso de auditoria lo que servirá como respaldo del proceso.

- ✓ **REPOSITORIO DE PRUEBAS:** Se divide en dos tipos de pruebas:

DE ANÁLISIS: Este espacio está destinado para describir las pruebas de análisis que se van a realizar para evaluar el proceso especifico que se encuentre en estudio.

DE EJECUCIÓN: Este espacio está destinado para describir las pruebas de ejecución que se van a realizar para evaluar el proceso especifico que se encuentre en estudio.

Tabla 2: Definición de fuentes de conocimiento, pruebas de análisis de auditoria

COACREMAT Ltda. Economía Solidaria de Altura	**CUADRO DE DEFINICION DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANALISIS DE AUDITORIA**	**REF**

ENTIDAD AUDITADA	Cooperativa del Magisterio de Túquerres	**PAGINA**		
		1	DE	1
DOMINIO AUDITADO	Planeación y Organización (PO)			
RESPONSABLE	José Alexander Melo I.			
MATERIAL DE SOPORTE	COBIT			

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANALISIS	**DE EJECUCION**

AUDITOR RESPONSABLE:
José Alexander Melo I.

- El Desarrollo de los cuestionarios cuantitativos se encuentran en el cd AUDITORIA DE SISTEMAS A COACREMAT en la carpeta CUADROS_DE_CONOCIMIENTO_CDFC

Cuestionario cuantitativo: El cuestionario cuantitativo permite dar una calificación numérica a un requerimiento dentro de los procesos que se estén auditando para determinar su vulnerabilidad.

Este cuestionario cuantitativo está conformado por los siguientes items:

REF: Se refiere al ID del elemento.

ENTIDAD AUDITADA: En este espacio se indicara el nombre de la entidad a la cual se le está realizando el proceso de auditoría.

PROCESO AUDITADO: En este espacio se indicara el nombre del proceso objeto de la auditoria, para el caso será Contratación TI.

RESPONSABLES: En este espacio se indicaran los nombres del equipo auditor que está llevando a cabo el proceso de auditoría.

DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: En este espacio se hace una breve referencia al objetivo del proceso seleccionado dentro de los dominios del COBIT que se está revisando.

MATERIAL DE SOPORTE: En este espacio se indicara el nombre del material que soporta el proceso, para el caso será COBIT.

DOMINIO: Espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.

PROCESO: Espacio reservado para el nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.

PREGUNTA: Espacio donde se indicara la descripción de la consulta de la cual se indagara.

SI – NO: Posibilidades de respuesta, cumple, no cumple, o no aplica para la entidad.

REF: referencia a la evidencia o el hallazgo que se obtuvo después de indagar.

PORCENTAJE DE RIESGO: Hace referencia a la probabilidad de que el proceso se vea afectado por las acciones de las cuales se está indagando, entre mas alto el porcentaje mayor probabilidad de riesgo tiene el proceso de salir perjudicado.

El cálculo de este porcentaje se hace de la siguiente forma:

Porcentaje de riesgo parcial = (Total SI * 100) / Total
Porcentaje de riesgo = 100 - Porcentaje de riesgo parcial

Las equivalencias utilizadas para la puntuación serán de uno a cinco, siendo uno el valor mínimo considerado de poca importancia y cinco el máximo considerado de mucha importancia.

Para determinar el nivel de riesgo total, se tiene en cuenta la siguiente categorización:

0% - 30% = Riesgo Bajo

31% - 70% = Riesgo Medio

71% - 100% = Riesgo Alto

Tabla 3: Cuestionario cuantitativo

COACREMAT Ltda. Economía Solidaria de Altura	**CUESTIONARIO CUANTITATIVO**	**REF**

ENTIDAD AUDITADA	Cooperativa del Magisterio de Túquerres - Coacremat			**PAGINA**	
				1	DE 1
PROCESO AUDITADO	Seguridad Lógica				
RESPONSABLE	José Alexander Melo I.				
MATERIAL DE SOPORTE		COBIT			
DOMINIO		**PROCESO**			

PREGUNTA	SI	NO	NA	REF	FUENTE
1. ¿?					
2. ¿?					

TOTALES			
TOTAL CUESTIONARIO			

PORCENTAJE DE RIESGO

AUDITOR RESPONSABLE
José Alexander Melo I.

- El Desarrollo de los cuestionarios cuantitativos en el cd AUDITORIA DE SISTEMAS A COACREMAT se encuentran en la carpeta de CUESTIONARIOS

Matriz de Probabilidad de ocurrencia e Impacto según relevancia del proceso

Esta matriz fue creada para catalogar un riesgo y saber qué clase de daño puede causar un mal procedimiento en el proceso auditado.

En la matriz existe la columna de probabilidad de ocurrencia donde se pondrá el valor del porcentaje de riesgo según su resultado.

Luego se deberá clasificar el impacto según la relevancia del proceso, esta clasificación será hecha por el equipo auditor basándose en el conocimiento de la entidad y del proceso auditado.

Una vez hechos estos procedimientos se podrá clasificar el riesgo para su posterior entendimiento.

Tabla 4: Matriz de probabilidad de ocurrencia e impacto según relevancia del proceso

PROBABILIDAD				
	ALTO 61-100%	**ZONA DE RIESGO MODERADO**	**ZONA DE RIESGO IMPORTANTE**	**ZONA DE RIESGO INACEPTABLE**
	MEDIO 31-60%	**ZONA DE RIESGO TOLERABLE**	**ZONA DE RIESGO MODERADO**	**ZONA DE RIESGO IMPORTANTE**
	BAJO 0-30%	**ZONA DE RIESGO ACEPTABLE**	**ZONA DE RIESGO TOLERABLE**	**ZONA DE RIESGO MODERADO**
		BAJO (LEVE)	**MEDIO (MODERADO)**	**ALTO (CATASTROFICO)**
	IMPACTO			

Manual de navegación de hallazgos. En este manual se describe las inconsistencias encontradas.

Esta información será desglosada de la siguiente manera:

REF: Se refiere al ID del elemento.

REF

HALLAZGOS	CH1 – PO2 **ENTIDAD AUDITADA (A):**

En este espacio se indicara el nombre de la entidad a la cual se le está realizando el proceso de auditoría.

PROCESO AUDITADO (B): En este espacio se indicara el nombre del proceso objeto de la auditoria, para el caso será Contratación TI.

RESPONSABLES (C): En este espacio se indicaran los nombres del equipo auditor que está llevando a cabo el proceso de auditoría.

MATERIAL DE SOPORTE (D): En este espacio se indicara el nombre del material que soporta el proceso, para el caso será COBIT.

DOMINIO (E): Espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.

PROCESO (F): Espacio reservado para el nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.

HALLAZGO: Aquí se encontrara la descripción de cada hallazgo, así como la referencia al cuestionario cuantitativo que lo soporta.

CONSECUENCIAS Y RIESGOS: En este apartado se encuentra la descripción de las consecuencias del hallazgo así como la cuantificación del riesgo encontrado.

EVIDENCIAS: Aquí se encuentra en nombre de la evidencia y el número del anexo donde ésta se encuentra.

RECOMENDACIONES: En este último apartado se hace una descripción de las recomendaciones que el equipo auditor ha presentado a las entidades auditadas.

Tabla 5: Hallazgos

	**HALLAZGO COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT**	**REF**

PROCESO AUDITADO	Datos	**PÁGINA**		
		1	DE	1
RESPONSABLE	José Alexander Melo I			
MATERIAL DE SOPORTE	COBIT			
DOMINIO		**PROCESO**		
HALAZGO:				
REF_PT:				
CONSECUENCIAS:				
RIESGO:				
RECOMENDACIONES:				

Resultado Matriz de probabilidad dominio planear y organizar (PO)

4.2.3 Hallazgos. A continuación se describen los hallazgos encontrados en la Cooperativa del Magisterio de Túquerres – Coacremat

4.2.3.1 Procesos Auditados en cooperativa del magisterio de Túquerres – Coacremat:

PROBABILIDAD				
	ALTO 61-100%			**H4 – PO9**
	MEDIO 31-60%		**H1 - PO2 H2 - PO3 H3 - PO4**	
	BAJO 0-30%			
		BAJO (LEVE)	**MEDIO (MODERADO)**	**ALTO (CATASTROFICO)**
	IMPACTO			

Los hallazgos encontrados en Coacremat son:

- **DOMINIO - PLANIFICACION Y ORGANIZACIÓN (PO)**

✓ PO2. Definir la Arquitectura de la Información

- ✓ PO3. Determinar la Dirección Tecnológica
- ✓ PO4. Definir los Procesos, Organización y Relaciones de TI
- ✓ PO9. Evaluar y Administrar los riesgos de TI

- **DOMINIO - ADQUIRIR E IMPLEMENTAR (AL)**

- ✓ AI2 Adquirir y Mantener Software Aplicativo
- ✓ AI3 Adquirir y Mantener Infraestructura Tecnológica
- ✓ AI4 Facilitar la Operación y el Uso
- ✓ AI6 Administrar Cambios

- **DOMINIO – ENTREGA DE SERVICIOS Y SOPORTE (DS)**

- ✓ DS3 Administrar el Desempeño y la Capacidad
- ✓ DS4 Garantizar la Continuidad del Servicio
- ✓ DS5 Garantizar la Seguridad de los Sistemas
- ✓ DS8 Administrar la Mesa de Servicio y los incidentes
- ✓ DS9 Administrar la Configuración
- ✓ DS10 Administración de Problemas
- ✓ DS11 Administración de Datos
- ✓ DS12 Administración del Ambiente físico

- **DOMINIO - MONITOREAR Y EVALUAR (ME)**

- ✓ ME1 Monitorear y Evaluar el Desempeño de TI

4.2.3.2 Hallazgos planificación y organización (PO):

PO2 Definir la arquitectura de la información: Los hallazgos o no conformidades encontradas se muestran en así:

Tabla 6: Hallazgo 1 ACMT

	**HALLAZGO COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT**	**REF** **CH1-PO2**

PROCESO AUDITADO	Datos	**PÁGINA**		
		1	DE	1
RESPONSABLE	José Alexander Melo I			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definir la Arquitectura de la Información (PO2)	

HALAZGO:

- En la Cooperativa del Magisterio de Túquerres – Coacremat no existe un procedimiento o software encargado de analizar los datos u archivos que se procesan en el sistema de información, estos datos fácilmente se pueden replicar en diferentes terminales, teniendo datos redundantes dentro de la Coacremat.
- No existe un software, diccionario de datos y esquema de clasificación de datos para eliminar datos redundantes que saturan al sistema de información puede que se eliminen datos que sean necesarios y se tengan datos almacenados que sean obsoletos dentro de los terminales de la empresa generando gasto en el espacio digital y volviendo al sistema redundante y lento.
- No existe un procedimiento o proceso de recuperación de archivos en línea ya que no se tiene unas políticas claras con respecto a este proceso, además Coacremat utiliza el internet como un medio de comunicación con las demás dependencias y sedes en diferentes partes del departamento de Nariño.

REF_PT: CD AUDITORIA DE SISTEMAS COACREMAT/CUESTIONARIOS/ CUESTIONARIO_1

CONSECUENCIAS:

- Incremento de trabajo: Ya que un mismo dato está almacenado en dos o más lugares, esto hace que cuando se graben o actualicen los datos, deban hacerse en todos los lugares a la vez.
- Desperdicio de espacio de almacenamiento: ya que los mismos datos están almacenados en varios lugares distintos, ocupando así más bytes del medio de almacenamiento.
- Inconsistencia de datos: Esto sucede cuando los datos redundantes no son iguales entre sí. Esto puede suceder, por ejemplo, cuando se actualiza el dato en un lugar, pero el dato duplicado en otro lugar no es actualizado.
- Al no existir un control de eliminación de datos redundantes que existen en Coacremat se puede caer en datos inconsistentes donde una persona puede alterar un dato que otra persona necesita, aumentando el incremento de trabajo.
- También se está colocando en riego la integridad de los datos ya que estos pueden cambiar los resultados de los procesos a los que son sometidos.
- Dificulta la tarea de modificación de datos y se genera una confusión con respecto al dato original generando información contradictoria o incongruente aumentando costos de almacenamiento.
- Perdida de información relevante para la Cooperativa del Magisterio de Túquerres dentro de la red de datos.
- Espera en la llegada de la información hacia las dependencias y sedes de la empresa.
- Tardanza en los procesos que utilizarían los archivos perdidos y no recuperados.

RIESGO:

- **Probabilidad de ocurrencia:** 54%
- **Impacto según relevancia del proceso:** Medio

RECOMENDACIONES:

- Realizar seguimientos a los datos que se tienen dentro del sistema de

información, teniendo un diccionario de datos y un esquema de clasificación de los mismos que sean propios de Coacremat.

- Implementar una política de reconocimiento de datos donde una persona sea la encargada de realizar la organización de datos para que sean organizados a través de un diccionario de datos y un esquema de clasificación de datos.
- Debe existir en todo el sistema procedimientos uniformes de validación para los datos ya que con esta validación se miraría los datos que son iguales y que se encuentran en dos o más lugares dentro del sistema de información para no generar duplicado de información es decir que la misma información sea más de una vez en un dispositivo de almacenamiento.
- Utilizar programas de recuperación de datos en línea
- Implementar un proceso de recuperación de datos y documentarlo para tener orden dentro de este procedimiento y para hacer las respectivas consultas cuando suceda algo parecido.

PO3 Determinar la dirección tecnológica: Los hallazgos o no conformidades encontradas se muestran en así:

Tabla 7: Hallazgo 2 ACMT

COACREMAT Ltda. Economía Solidaria de Altura	**HALLAZGO COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT**	**REF**
		CH2-PO3

PROCESO AUDITADO	Infraestructura Tecnológica	**PÁGINA**		
		1	DE	1
RESPONSABLE	José Alexander Melo I			

MATERIAL DE SOPORTE	COBIT		
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Determinar la Dirección Tecnológica (PO3)

HALAZGO:

No existe políticas de evaluación de desempeño y calidad dentro de Coacremat, para medir la eficacia de los procesos que utilizan la plataforma tecnológica, evaluando los objetivos ejecutados y realizados identificando posibles anomalías y puntos críticos dentro del sistema de información y periódico donde se estimar cuantitativa y cualitativamente el grado de eficacia y eficiencia de cada uno de los procesos.

REF_PT: CD AUDITORIA DE SISTEMAS COACREMAT/CUESTIONARIO / CUESTIONARIO_2

CONSECUENCIAS:

- Reducción de cantidad y calidad dentro de los procesos porque no se han identificado posibles vulnerabilidades por falta de la evaluación del desempeño.
- Incremento de problemas que se encuentran afectando a los procedimientos del sistema de información.

RIESGO:

Probabilidad de ocurrencia:$= 42\%$
Impacto según relevancia del proceso: Medio

RECOMENDACIONES:

- Realizar procesos y políticas de autoevaluación de desempeño y calidad al sistema de información en su plataforma tecnológica.
- Aplicar estándares de desempeño y calidad dentro de la autoevaluación haciendo un modelado del sistema de información aplicando diferentes pruebas y sus consecuencias.

PO4 Definir los procesos, organización y relaciones de TI: Los hallazgos o no conformidades encontradas se muestran en así:

Tabla 8: Hallazgo 3 ACMT

<table>
<tr><td></td><td colspan="3">HALLAZGO COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT</td><td>REF

CH3-PO4</td></tr>
<tr><td>PROCESO AUDITADO</td><td colspan="2">Seguridad Física de Coacremat</td><td>PÁGINA
1 DE 1</td></tr>
<tr><td>RESPONSABLE</td><td colspan="3">Organización y comunicación TI</td></tr>
<tr><td>MATERIAL DE SOPORTE</td><td colspan="3">COBIT</td></tr>
<tr><td>DOMINIO</td><td>Planeación y Organización (PO)</td><td>PROCESO</td><td>Definir los Procesos, Organización y Relaciones de TI (P04)</td></tr>
<tr><td colspan="4">HALLAZGO:
• No se cuenta con una persona encargada de la seguridad en el edificio.
• Dentro de las políticas de seguridad no se considera el servicio de celaduría para evitar posibles desmandes por parte de actores armados.
• No existe un control de las personas que acceden al departamento de sistemas que es de donde se maneja el sistema de información linix.
• Cualquier persona puede ingresar sin una credencial o permiso por parte de la cooperativa.</td></tr>
<tr><td colspan="4">REF_PT: CD AUDITORIA DE SISTEMAS COACREMAT/CUESTIONARIO / CUESTIONARIO_3</td></tr>
<tr><td colspan="4"></td></tr>
</table>

CONSECUENCIAS:

- Inseguridad dentro de la organización.
- No se puede controlar la entrada, salida de personas y el porte de armas, ya sea arma blanca o armamento no autorizado por la empresa.
- Fácil robo de elementos de información de la cooperativa ya sean actores internos o externos.
- Puede ingresar cualquier persona sin previa autorización.
- Se puede hurtar archivos o información de la empresa y ser mal utilizada por parte de personas mail intencionadas.

RIESGO:

Probabilidad de ocurrencia: $= 52\%$
Impacto según relevancia del proceso: Medio

RECOMENDACIONES:

- Tener una política de seguridad física para la empresa que ejerza el control, inspección y vigilancia sobre de la cooperativa.
- Realizar un estudio sobre lo necesario de que una empresa de seguridad se encargue de adoptar las buenas normas de seguridad dentro de Coacremat.
- Realizar simulacros de infiltración de ladrones para mirar las vulnerabilidades de la empresa y que lugares son más seguros dentro de ella.
- Investigar al personal encargado de la seguridad.
- Realizar un servicio de identificación en la puerta.
- Adoptar políticas de seguridad para la implementación de procesos de seguridad que beneficien a la empresa y que siempre se encuentren disponibles.

PO4 Evaluar y administrar los riesgos de TI: Los hallazgos o no conformidades encontradas se muestran en así:

Tabla 9: Hallazgo 4 ACMT

COACREMAT Ltda. Economía Solidaria de Altura	**HALLAZGO COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT**	**REF** **CH1-PO9**

PROCESO AUDITADO	Seguridad Física	**PÁGINA** 1 DE 1		
RESPONSABLE	Organización y comunicación TI			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Evaluar y Administrar los riesgos de TI (P09)	

HALAZGO:

- Coacremat no cuenta con planes de contingencia antes riesgos potenciales que se pueden dar sin previo aviso.
- No existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo.
- No se registra el acceso al cuarto de servidores de personas ajenas a la dirección de sistemas
- No existe alarma para detectar condiciones anormales del ambiente en el cuarto del servidor.

REF_PT: CD AUDITORIA DE SISTEMAS COACREMAT/CUESTIONARIO / CUESTIONARIO_5

CONSECUENCIAS:

- No tener una buena gestión para el buen gobierno de las tecnologías de la información y las comunicaciones dentro de la empresa.
- Las amenazas no serían identificadas en plenitud y el impacto hacia la empresa sería catastrófico e impediría su normal funcionamiento.
- No se realizaría una revisión y reparación a los equipos de cómputo como a las instalaciones que garanticen su buen funcionamiento y fiabilidad.
- Al no registrar al personal que ingrese al cuarto de servidores, estos podrían realizar cualquier tipo de manipulación a la parte física considerado como un saboteo.
- Se podría robar información violando contraseñas y podría extraer equipos que perjudiquen el normal funcionamiento de los servidores.
- Las condiciones de un cuarto para servidores deben tener unas especificaciones especiales, una de ellas es la implementación de una alarma para detectar condiciones anormales dentro del cuarto de servidores para lograr una mayor eficacia en cuanto a la protección de este sitio.

RIESGO:

Probabilidad de ocurrencia: $= 74\%$
Impacto según relevancia del proceso: Alto

RECOMENDACIONES:

- Implementar políticas desde la gerencia para realizar un plan de amenazas que Coacremat puede tener, debe ser documentado para utilizarlo posteriormente donde se encuentren la amenaza que tipo de daño le haría a la empresa y el impacto a los procesos de la cooperativa.
- Elaborar el plan de contingencia que permita conocer puntos críticos en la empresa para garantizar un buen funcionamiento de la misma, logrando prevenir las incidencias antes de que estas ocurran.
- Elaborar e implementar un plan de mantenimiento de conservación como correctivo y preventivo que traten de ajustarse a la empresa para lograr un funcionamiento eficaz para obtener mejores resultado y no tener contratiempos en los procesos de Coacremat, también implantar un plan de mantenimiento de actualización para las aplicaciones o programas que

lo requieran sin interferir en las configuraciones de los diferentes dispositivos.

- Elaborar una política de seguridad para el cuarto de servidores para mejorar la protección a saboteos y robo de dispositivos o de información.
- Realizar un estudio para implementar y mejorar el cuarto de servidores para que tenga las normas técnicas para alojar dichas maquinas.

4.2.3.2 Resultado Matriz de probabilidad dominio Adquirir e implementar (AL)

PROBABILIDAD				
	ALTO 61-100%			**H3-AL4**
	MEDIO 31-60%	**H3 – AL6**	**H1 - AL2 H2 – AL3**	
	BAJO 0-30%			
		BAJO (LEVE)	**MEDIO (MODERADO)**	**ALTO (CATASTROFICO)**
	IMPACTO			

4.2.3.3 Hallazgos dominio: adquirir e implementar (AL). A continuación se describirán los hallazgos encontrados en la Cooperativa del Magisterio de Túquerres – Coacremat.

AI2 Adquirir y mantener software aplicativo: Los hallazgos o no conformidades encontradas se muestran en así:

Tabla 10: Hallazgo 1 ACMT

COACREMAT Ltda. Economía Solidaria de Altura	**HALLAZGO COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT**	**REF** **CH1-AL2**

PROCESO AUDITADO	Software		**PÁGINA** 1 DE 1		
RESPONSABLE	Organización y comunicación TI				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquirir E Implementar (AL)	**PROCESO**	Adquirir y Mantener Software Aplicativo (AL)		
Hallazgo • No existe un plan de gestión de riesgos de seguridad de las aplicaciones aprobado por la dirección • No se han desarrollado aplicaciones para complementar el software empresarial • La empresa no cuenta con un plan de aseguramiento de calidad de software • La empresa no cuenta con una estrategia y un plan de mantenimiento de					

software

REF_PT: CD AUDITORIA DE SISTEMAS COACREMAT/CUESTIONARIO / CUESTIONARIO_6

CONSECUENCIAS:

- Evasión de los riesgos que potencialmente se pueden convertir en desastre.
- Menor tiempo de reacción ante un riesgo.
- Incertidumbre en la empresa porque no se sabe a qué tipo de riesgos se está enfrentando.
- El desarrollo de aplicaciones hace que los procesos sean más eficaces ya que a través de estas se logra abarcar mayor cantidad de trabajo disminuyendo costos de tiempos.
- No se hacen pruebas de software con el objetivo de disminuir el riesgo de la ocurrencia de fallas al implementar, instalar o actualizar sistemas en producción, teniendo en cuenta la criticidad del sistema actual.
- Al no realizar un plan de mantenimiento de software los problemas que puedan suceder dentro de las aplicaciones pueden generar demoras y pérdidas de datos.

RIESGO:

Probabilidad de ocurrencia: $= 42\%$
Impacto según relevancia del proceso: Medio

RECOMENDACIONES:

- Implementar políticas desde la gerencia para la gestión de riesgos para el software ya que se debe interactuar con estos programas que deben ser probados antes de ser implantados en la plataforma tecnológica así contribuyendo a mejorar la calidad del software y la satisfacción del cliente, volviendo los sistemas más confiables para el usuario final.
- Implementar políticas de desarrollo de software empresarial desde el departamento de sistemas que ayude a soportar algunos procesos y sea de ayuda y se integre con el sistema linix.

- Implementar un plan de aseguramiento de calidad de software donde se realicen pruebas como de sistemas, integración y aceptación del software que se desea ejecutar para disminuir problemas de incompatibilidad de software que potencialmente pueden perjudicar la información de la empresa.
- Implementar unas políticas donde se implementen programas y estrategias de planes de mantenimiento.

AI3 Adquirir y mantener infraestructura tecnológica: Los hallazgos o no conformidades encontradas se muestran en así:

Tabla 11: Hallazgo 2 ACMT

COACREMAT Ltda. Economía Solidaria de Altura	**HALLAZGO COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT**	**REF**
		CH2-AL3

PROCESO AUDITADO	Infraestructura Tecnológica	**PÁGINA**		
		1	DE	1
RESPONSABLE	José Alexander Melo I			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquirir E Implementar (AL)	**PROCESO**	Adquirir y Mantener Infraestructura Tecnológica(Al3)	

HALAZGO:

- No se tienen repuestos importantes, y actualizan este stock, en almacén.
- No se tienen planes con los equipos que han terminado su ciclo de vida.

REF_PT: CD AUDITORIA DE SISTEMAS COACREMAT/CUESTIONARIO / CUESTIONARIO_7

CONSECUENCIAS:

- El no tener un almacén en la cooperativa con dispositivos de importancia para ciertos equipos hace de que los procesos por parte de equipos dañados sean lentos y algunas veces hace de que sean cancelados por parte de los administradores.
- Cumulo de basura electrónica dentro de la empresa en espacios no adecuados para mantener estos equipos electrónicos generando toxicidad y posibles cortos electrónicos generando incendios y contaminación.

RIESGO:

Probabilidad de ocurrencia: $= 59\%$
Impacto según relevancia del proceso: Medio

RECOMENDACIONES:

- Implementar un almacén donde se encuentren dispositivos de alta necesidad para la infraestructura tecnológica para garantizar un adecuado remplazo y así no generar una parálisis en os procesos.
- Implementar políticas de basura electrónica con equipos desactualizados donde se pueden incorporar a ciertas áreas y tomar las medidas adecuadas para que esos aparatos electrónicos sean desechados de manera correcta.

AI4 Facilitar la operación y el uso: Los hallazgos o no conformidades encontradas se muestran en así:

Tabla 12: Hallazgo 3 ACMT

COACREMAT Ltda. Economía Solidaria de Altura	**HALLAZGO COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT**	**REF** **CH3-AL4**

PROCESO AUDITADO	Manuales de software	**PÁGINA** 1 DE 1		
RESPONSABLE	José Alexander Melo I			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquirir E Implementar (AL)	**PROCESO**	Facilitar la Operación y el Uso (AL4)	

HALAZGO:

- No se ha creado un documento donde se pueda identificar los aspectos técnicos, la capacidad de operación y los niveles de servicio de os diferentes programas que se encuentra usando la empresa.

REF_PT: CD AUDITORIA DE SISTEMAS COACREMAT/CUESTIONARIO / CUESTIONARIO_8

CONSECUENCIAS:

- El mal uso del software por parte de las personas que manipulan estos programas.
- Desconocimiento de para qué sirve el software y en que procesos lo puede utilizar generando una subutilización del programa.
- Se genera desconfianza en el trabajador bajando el nivel de trabajo para la empresa, creando errores humanos que perjudicarían a la cooperativa.

RIESGO: **Probabilidad de ocurrencia:**= 83% **Impacto según relevancia del proceso:** Alto
RECOMENDACIONES: • Implementar un manual de usuario para las personas que manipulan los diferentes programas de la cooperativa donde se encontraría el uso de los programas y la solución de problemas que puedan suceder en la operación logrando disminuir los errores humanos que son unas de las principales causas para que el trabajo no sea óptimo.

AI6 Facilitar la operación y el uso: Los hallazgos o no conformidades encontradas se muestran en así:

Tabla 13: Hallazgo 4 ACMT

COACREMAT Ltda. Economía Solidaria de Altura	**HALLAZGO COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT**	**REF** **CH4-AL6**

PROCESO AUDITADO	Solicitud de cambios	**PÁGINA**		
		1	DE	1
RESPONSABLE	José Alexander Melo I			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquirir E	**PROCESO**	Administrar	

	Implementar (AL)		Cambios (AI6)

HALAZGO:

- No se cuenta con un sistema o proceso que realice seguimiento y reporte a las solicitudes de cambio en el sistema de información.

REF_PT: CD AUDITORIA DE SISTEMAS COACREMAT/CUESTIONARIO / CUESTIONARIO_10

CONSECUENCIAS:

- Desorganización de las diferentes peticiones y solicitudes de cambio en el sistema de información.

RIESGO:

Probabilidad de ocurrencia:$= 36\%$
Impacto según relevancia del proceso: Medio

RECOMENDACIONES:

- Implementar políticas para contar con un sistema de gestión de solicitudes de cambio, esto se lo puede hacer a través de un desarrollo de software para la cooperativa.

4.2.3.4 Resultado matriz de probabilidad dominio entregar y dar soporte (DS)

PROBABILIDAD				
	ALTO 61-100%			H1 – DS3 H2 – DS4 H4 – DS8 H8 – DS12
	MEDIO 31-60%		H3 – DS5 H5 – DS9 H7 – DS11 H6 - D10	
	BAJO 0-30%			
		BAJO (LEVE)	MEDIO (MODERADO)	ALTO (CATASTROFICO)
	IMPACTO			

4.2.3.5 Hallazgos entregar y dar soporte (DS). A continuación se describirán los hallazgos encontrados en la Cooperativa del Magisterio de Túquerres – Coacremat

DS3 Administrar el desempeño y la capacidad: Los hallazgos o no conformidades encontradas se muestran en así:

Tabla 14: Hallazgo 1 ACMT

	**HALLAZGO COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT**	**REF**
		CH1-DS3

PROCESO AUDITADO	Desempeño del sistema		**PÁGINA**	
			1 DE 1	
RESPONSABLE	José Alexander Melo I			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entregar y dar Soporte (DS)	**PROCESO**	Administrar el Desempeño y la Capacidad (DS3)	

HALAZGO:

- No se evalúa el desempeño y la capacidad del sistema de información linix.
- No existe un software o un mecanismo estadístico, que pueda dar respuesta, al desempeño actual en los procesos del sistema en toda la organización.
- No existen reuniones semanales o quincenales, por el departamento de sistemas para evaluar, los incidentes y procesos, en los cuales están a cargo.
- No se tiene respaldo de información en un servidor espejo.

REF_PT: CD AUDITORIA DE SISTEMAS COACREMAT/CUESTIONARIO / CUESTIONARIO_11

CONSECUENCIAS:

- Al no existir una evaluación al sistema de información linix sobre la capacidad de registro de los datos y errores que presenta algunas veces se pierde la definición de objetivos del sistema de información, ya que los errores que este software posea seguirán creciendo y no se sustentaría en ningún reporte de evaluación de desempeño.
- Al no existir un programa o procedimiento organizativo que contenga los diferentes procesos que se manejan en la empresa para evaluar el desempeño, no se tendría una idea de cómo estas tecnologías están trabajando sin importar los errores que puedan tener sin obtener una estadística que se la puede usar para el beneficio del sistema.
- Al no existir unas reuniones informativas que retroalimenten la situación de posibles errores dentro del sistema no se tendría conocimiento de las posibles vulnerabilidades que se pueden registrar en los procesos.
- Si por alguna razón sucede una catástrofe como factores naturales y humanos en la sede central de Coacremat que es donde se congrega la mayor cantidad de información, estos no se los podría recuperar ya que sin un servidor espejo que se encuentre en otro lugar diferente a la sede para albergar la información y hacer copias de seguridad diarias para soportar posibles dificultades que se puedan presentar.

RIESGO:

Probabilidad de ocurrencia:= 72%
Impacto según relevancia del proceso: Alto

RECOMENDACIONES:

- Elaborar e implementar unas políticas de evaluación de la capacidad del sistema linix donde le proveedor puede colaborar a través de sus registros y al final se consolidaría la información para tener una autoevaluación de los procesos que maneja el sistema linix.
- Implementar un procedimiento o programa que gestione los datos de las evaluaciones para sacar estadísticas que servirán en un futuro ya que ellas muestran los posibles errores que pueden suceder a futuro.
- Implementar un cronograma de reuniones ya sean semanales o mensuales para verificar los datos de las evaluaciones de rendimiento de los procesos que tiene a cargo el sistema de información.
- Implementar un programa para encontrar respuesta a esta situación, no

solo puede ser un servidor espejo, se puede guardar datos en la nube o albergar los backaps en otro lugar diferente a la sede central.

DS4 Garantizar la continuidad del servicio: Los hallazgos o no conformidades encontradas se muestran en así:

Tabla 15: Hallazgo 2 ACMT

COACREMAT Ltda. Economía Solidaria de Altura	**HALLAZGO COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT**	**REF** **CH2-DS4**

PROCESO AUDITADO	Continuidad del servicio		**PÁGINA** 1 DE 1	
RESPONSABLE	José Alexander Melo I			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entregar y dar Soporte (DS)	**PROCESO**	Garantizar la Continuidad del Servicio (DS4)	

HALAZGO:

- No se llevan a cabo pruebas de los procedimientos de recuperación de datos.
- No existen procedimientos para asegurar que las copias están adecuadamente protegidas y solo disponibles para el personal especialmente autorizado
- Actualmente la organización no posee alguna alternativa que permita la continuidad del desarrollo de los procesos normales, luego de una falla total en el sistema principal.

- No existe un repositorio de información sobre desastres ocurridos anteriormente que provean un panorama para posibles errores a futuro.
- No se lleva a cabo dentro de la organización algún tipo de registro sobre los errores más comunes, que permita un análisis de probabilidad de ocurrencia de fallas.
- Las personas que trabajan en la cooperativa no conocen los planes de continuidad para que el sistema trabaje de forma óptima.

REF_PT: CD AUDITORIA DE SISTEMAS COACREMAT/CUESTIONARIO / CUESTIONARIO_12

CONSECUENCIAS:

- Al no hacer pruebas de recuperación de datos no se estará preparado para eventuales catástrofes donde se requiere hacer este ejercicio por lo tanto no se tendría conocimiento de cómo actuar en una situación de siniestros de la cooperativa.
- Las copias de seguridad son activos digitales de la empresa donde cualquier persona puede acceder a ellos provocando una indagación de personas no autorizadas a estos archivos.
- No existe un procedimiento o manual que permita verificar ¿Que hacer en caso de una catástrofe donde se paran todos los procesos del sistema de información? para que continúe con un norma funcionamiento sin que los usuarios se den cuenta de este hecho.
- Al no tener un manual donde se observen los errores y posibles soluciones ocurridos anteriormente no se contara con un soporte técnico para dar solución a problemas que se puedan dar en un futuro.
- El desconocimiento de un plan de continuidad hace que el personal se confunda cuando suceda un problema con el sistema de información.

RIESGO:

Probabilidad de ocurrencia:= 75%
Impacto según relevancia del proceso: Alto

RECOMENDACIONES:

- Establecer un cronograma de pruebas de recuperación de datos donde se simule una situación donde implique utilizar este proceso de recuperación de datos.

- Implementar unas políticas de seguridad para salvaguardar las diferentes copias de seguridad existentes en la cooperativa del magisterio de Túquerres para que estas puedan ser utilizadas en una catástrofe que pueda ocurrir dentro de la cooperativa.
- Implementar un manual donde se encuentre que hacer después de una falla total del sistema de información que sirva de guía para futuras consultas.
- Elaborar un repositorio documentado de desastres ocurridos en la cooperativa donde se registren los problemas más comunes, ya que este será una guía para problemas que se pueden repetir en un futuro.
- Elaborar un manual para las personas que desconozcan los planes de continuidad del sistema de información o cualquiera de sus componentes para que sea utilizados los planes de contingencia de una forma correcta y no caer en errores humanos.

DS5 Garantizar la seguridad de los sistemas: Los hallazgos o no conformidades encontradas se muestran en así:

Tabla 16: Hallazgo 3 ACMT

COACREMAT Ltda. Economía Solidaria de Altura	**HALLAZGO COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT**	**REF** **CH3-DS5**

PROCESO AUDITADO	Seguridad Lógica	**PÁGINA** 1	DE	1
RESPONSABLE	José Alexander Melo I			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entregar y dar	**PROCESO**	Garantizar la Seguridad de los	

	Soporte (DS)		Sistemas (DS5)

HALAZGO:

- No se tiene planes de seguridad de TI implementados en la empresa.
- No se tienen identificado los riesgos que pueden interferir en el sistema de información.
- No se cuenta con un documento o plan de seguridad dentro de la cooperativa.
- Las copias de seguridad de los datos no cuentan con claves de acceso.

REF_PT: CD AUDITORIA DE SISTEMAS COACREMAT/CUESTIONARIO / CUESTIONARIO_13

CONSECUENCIAS:

- No se cuenta con normas y procedimientos de la seguridad de la información digital de la empresa, ni se analiza la necesidad de cambios ni adaptaciones para cubrir los riesgos existentes.
- Al no existir normas sobre cómo actuar ante una posible vulnerabilidad tanto interna como externa no se cuenta con una identificación de riesgos, estos pueden hacer que el sistema de información colapse en cualquier momento.
- Las copias de seguridad deben protegerse mediante contraseñar para evitar la manipulación, solo el personal autorizado lo debe hacer para evitar posibles daños en la información.

RIESGO:

Probabilidad de ocurrencia: $= 50\%$
Impacto según relevancia del proceso: Medio

RECOMENDACIONES:

- Implementar políticas gerenciales para construir un plan de seguridad informática que satisfaga las necesidades de los sistemas de información de Coacremat así como cada uno de los componentes que son parte de este para qué se pauten las actividades relacionadas con la seguridad informática.

• Al implementar las políticas de seguridad informática elaborar un documento con los puntos críticos del sistema de información, identificando posibles vulnerabilidades en el sistema. • Colocar clave a las copias de seguridad para que proteja la integridad de los datos que se encuentran en estos dispositivos.

DS8 Administrar la mesa de servicio y los incidentes: Los hallazgos o no conformidades encontradas se muestran en así:

Tabla 17: Hallazgo 4 ACMT

COACREMAT Ltda. Economía Solidaria de Altura	**HALLAZGO COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT**	**REF** **CH4-DS8**

PROCESO AUDITADO	Incidentes		**PÁGINA**		
			1	DE	1
RESPONSABLE	José Alexander Melo I				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y dar Soporte (DS)	**PROCESO**	Administrar la Mesa de Servicio y los incidentes(DS8)		
HALAZGO: • En la empresa no se registra los diferentes incidentes que se pueden presentar. • No se llevan registros de las consultas realizadas por los usuarios (registro y rastreo de llamadas, incidentes, solicitudes de servicio y					

necesidades de información).
REF_PT: CD AUDITORIA DE SISTEMAS COACREMAT/CUESTIONARIO/ CUESTIONARIO_15
CONSECUENCIAS: • Al no registrar los incidentes informáticos del sistema de información de Coacremat los eventos ocurridos anteriormente no se tendrían en cuanta para lograr un óptimo desempeño de los componentes del sistema para lograr una producción de trabajo que sea eficaz y confiable en Coacremat. • Al no existir un registro de las diferentes de las consultas, incidentes de servicio y necesidades de información por parte de los usuarios, se desconocería como el sistema está funcionando y que errores se están llevando a los usuarios.
RIESGO: **Probabilidad de ocurrencia:**= 77% **Impacto según relevancia del proceso:** Alto
RECOMENDACIONES: • Elaborar e implementar políticas y procesos donde se registren los incidentes informáticos de los diferentes componentes de los sistemas de información para obtener unos datos y hacer un seguimiento para mejorar el servicio. • Implementar políticas de registros de incidentes, elaborando un manual donde el usuario pueda participar de los diferentes incidentes que le suceda en el sistema de información.

DS9 Administrar la configuración: Los hallazgos o no conformidades encontradas se muestran en así:

Tabla 18: Hallazgo 5 ACMT

	HALLAZGO COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT	**REF**
		CH5-DS9

PROCESO AUDITADO	Configuración		**PÁGINA**	
			1 DE 1	
RESPONSABLE	José Alexander Melo I			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entregar y dar Soporte (DS)	**PROCESO**	Administrar la Configuración (DS9)	

HALAZGO:

- No existe un responsable encargado de la gestión de la configuración de los diferentes terminales.
- No existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo.
- La cooperativa no tiene un plan de mantenimiento y configuración de los dispositivos, y no está documentado.

REF_PT: CD AUDITORIA DE SISTEMAS COACREMAT /CUESTIONARIOS/ CUESTIONARIO_16

CONSECUENCIAS:

- Al no existir un manual de funciones bien definido y con unas tares bien definidas para cada usuario, no existirá una persona que realice y verifique la configuración de cada terminal.

- Al no realizar un mantenimiento preventivo a los diferentes equipos de la cooperativa se corre el riesgo de que estos dispositivos fallen en un tiempo corto ya que no se solucionarían problemas ni se los previene, para que no sucedan problemas con los equipos.
- Al no tener un documento donde se encuentren cronogramas, la configuración de los equipos no se tendrá claridad con la información que tienen las terminales.

RIESGO:

Probabilidad de ocurrencia:$= 52\%$
Impacto según relevancia del proceso: Medio

RECOMENDACIONES:

- Implementar un manual de funciones donde se encuentren las tareas bien definidas con su perfil profesional par que cada persona realice las tareas asignadas.
- Implementar un mantenimiento preventivo cada mes para prevenir posibles errores cuando el sistema esté en producción.
- Realizar planes de mantenimiento a todo el sistema de información con documentación para lograr una mejor optimización de los dispositivos que conforman el sistema.

DS10 Administración de problemas: Los hallazgos o no conformidades encontradas se muestran en así:

Tabla 19: Hallazgo 6 ACMT

COACREMAT Ltda. Economía Solidaria de Altura	**HALLAZGO COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT**	**REF** **CH6-DS10**

PROCESO AUDITADO	Categorización de problemas o incidentes.		**PÁGINA** 1 DE 1	
RESPONSABLE	José Alexander Melo I			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entregar y dar Soporte (DS)	**PROCESO**	Administración de Problemas (DS10)	

HALAZGO:

- Los problemas que se reportan no son categorizados.
- Los problemas no son documentados para tener un registro y posteriormente utilizarlos para resolver un incidente.

REF_PT: CD AUDITORIA DE SISTEMAS COACREMAT / CUESTIONARIO/ CUESTIONARIO_17

CONSECUENCIAS:

- Al no reportar los problemas y no categorizarlos en un documento, estos pasarían desapercibidos y provocarían problemas al sistema más adelante sin tener conocimiento de que tipo de problema está sucediendo en el sistema de información obligando muchas veces a reiniciar el sistema y deteniendo procesos vitales para la cooperativa.
- Si los problemas no son documentados no se sabe qué tipo de daño le hicieron al sistema de información y cuál fue su solución.

RIESGO: **Probabilidad de ocurrencia:**= 67% **Impacto según relevancia del proceso:** Medio
RECOMENDACIONES: • Implementar un documento donde se reporten las diferentes incidencias del sistema de información para categorizarlos y analizar sus resultados para tomar decisiones con respecto al problema que se haya encontrado. • Implementar políticas gerenciales que ayuden a tomar decisiones con respecto al os problemas que suceden en el sistema de información.

DS11 Administración de datos: Los hallazgos o no conformidades encontradas se muestran en así:

Tabla 20: Hallazgo 7 ACMT

COACREMAT Ltda. Economía Solidaria de Altura	**HALLAZGO COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT**	**REF** **CH7-DS11**

PROCESO AUDITADO	Administración de datos	**PÁGINA**		
		1	DE	1
RESPONSABLE	José Alexander Melo I			
MATERIAL DE SOPORTE	COBIT			

DOMINIO	Entregar y dar Soporte (DS)	**PROCESO**	Administración de Datos (DS11)

HALAZGO:

- No verifican que las copias de seguridad sean iguales, ósea que la integridad de los datos iguales a las originales.
- No se tienen procedimientos que permitan la reconstrucción de un archivo digital, el cual fue inadvertidamente destruido.
- No existe un control estricto de las copias de seguridad.

REF_PT: CD AUDITORIA DE SISTEMAS COACREMAT / CUESTIONARIO/ CUESTIONARIO_18

CONSECUENCIAS:

- Al no verificar la integridad de datos de las copias de seguridad, estas se las puede utilizar de forma errónea dando resultados diferentes en los procesos involucrados.
- Al no tener un proceso para recuperar un archivo que no ha sido guardado previamente, se puede perder información importante de la empresa retrasando la toma de decisiones de la cooperativa.
- Al no existir un control a las copias de seguridad cualquier persona puede manipular y sacar información de la cooperativa sin autorización.

RIESGO:

Probabilidad de ocurrencia: $= 66\%$

Impacto según relevancia del proceso: Medio

RECOMENDACIONES:

- Implementar una verificación de datos en las copias de seguridad para verificar posibles alteraciones a esta información.
- Implementar un software que permita recuperar un archivo en caso de que este se haya borrado de forma accidental.
- Implementar un controla las copias de seguridad para que estas sean utilizadas exclusivamente por personal autorizado.

DS12 Administración del ambiente físico: Los hallazgos o no conformidades encontradas se muestran en así:

Tabla 21: Hallazgo 8 ACMT

COACREMAT Ltda. Economía Solidaria de Altura	**HALLAZGO COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT**	**REF** **CH8-DS12**

PROCESO AUDITADO	Ambiente Físico		**PÁGINA**		
			1	DE	1
RESPONSABLE	José Alexander Melo I				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y dar Soporte (DS)	**PROCESO**	Administración del Ambiente físico (DS12)		

HALAZGO:

- No existen una persona responsable de la seguridad
- No existe personal de vigilancia en la institución
- No existe vigilancia en el cuarto del servidor
- Se permite el acceso a los archivos y programas al personal de la cooperativa sin importar su rol
- No se ha instruido al personal sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización
- No existen extintores de fuego
- Los interruptores de energía no están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos
- No existe salida de emergencia

REF_PT: CD AUDITORIA DE SISTEMAS COACREMAT / CUESTIONARIO

/CUESTIONARIO_19

CONSECUENCIAS:

- Al no existir un vigilante en la empresa personal no autorizado podría entrar a robar sin ningún obstáculo.
- Al no existir un sistema de vigilancia en el cuarto de servidor lo podrían manipular para robar información o podrían robar dispositivos importantes como discos duros sin que nadie lo note.
- Al permitir que las demás personas miren información que no les compete podrían causar daños en el archivo, modificando su información.
- Al no instruir al personal sobre la posible entrada de personas desconocidas con fines de robo estas podrían alterarse de forma nerviosa habiendo accidentes no deseados para la empresa.
- Al no existir extintores de fuego a mano una simple llama se podría convertir en un gran incendio.
- Al no existir interruptores de energía debidamente etiquetados cualquier persona podría confundir y hacer un corto circuito que dañaría los equipos de Coacremat.
- Al no existir una salida de emergencia para siniestros naturales o humanos, las puertas podrían acumular gente sin que nadie pueda salir a un lugar protegido.

RIESGO:

Probabilidad de ocurrencia:= 79%

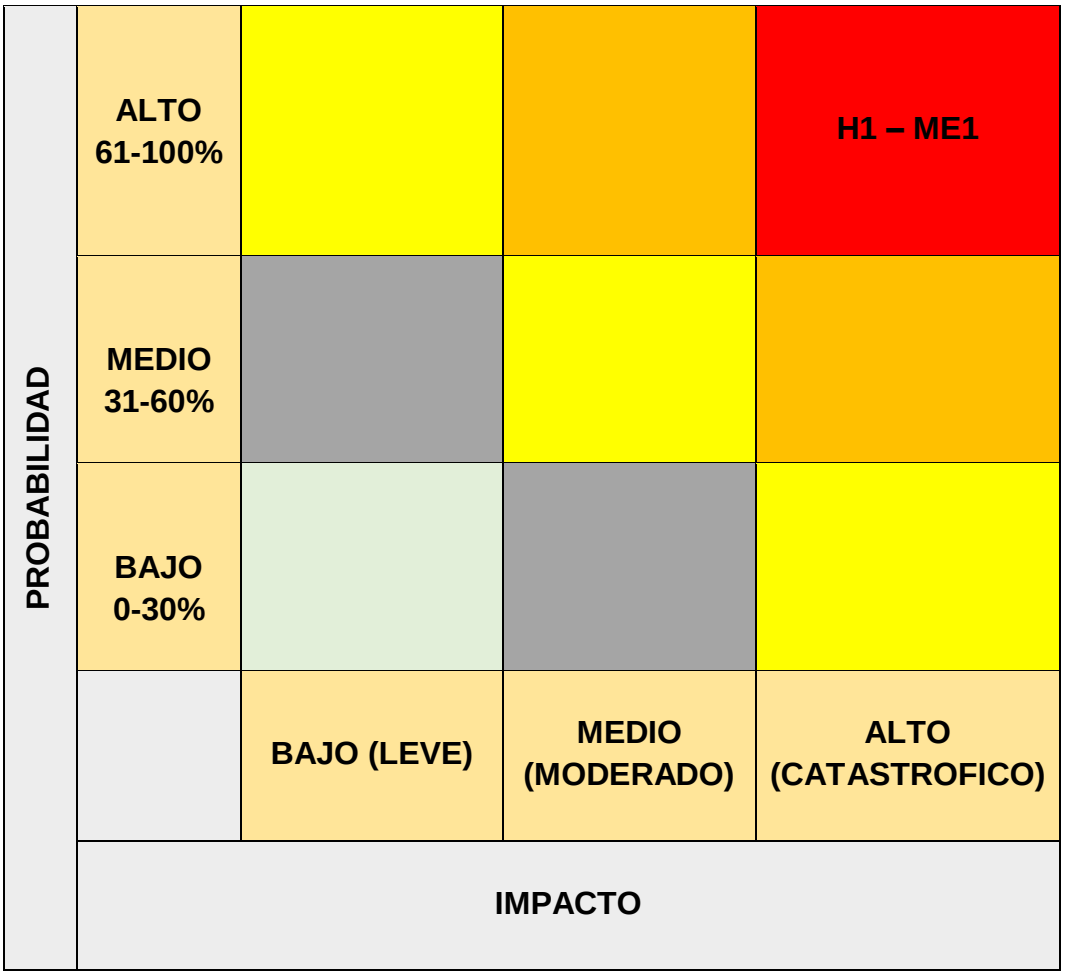
Impacto según relevancia del proceso: Alto

RECOMENDACIONES:

- Implementar políticas de seguridad física que comprometa a la gerencia para contrata una persona idónea y con responsabilidad para la vigilancia del edificio.
- Implantar un sistema de monitoreo para el cuarto del servidor, pueden ser cámaras o sensores de movimientos que informen al encargado de este lugar que existen personas no autorizadas manipulando el cuarto de servidores.

- Utilizar un programa o crear roles de usuarios donde no se permita ver archivos de otras personas y tener cuidado con los comandos que permiten mirar archivos en cualquier parte del sistema de información, estos no deben ser suministrados a ninguna persona.
- Implementar simulacros donde puedan verificar el estado psicológico de cada persona para afrontar posible amenazas como la entrada de personas que tengan intenciones de robar, para que así el personal este más atento y maneje un proceso que se ira creando según la necesidad de la cooperativa.
- Adquirir extintores de fuego para neutralizar posibles incendios, estos deben estar a la mano y muy cerca de puntos que sean posibles focos de incendios.
- Etiquetar los interruptores de energía para saber que voltaje tienen y tratar de que estos no sean obstaculizados por objetos que no dejen mirar que tipo de conector es.
- Implementar una salida de emergencia para que permita una rápida evacuación del edificio en caso de catástrofes naturales.

4.2.3.6 Resultado matriz de probabilidad dominio monitorear y evaluar (ME)



4.2.3.7 Hallazgos monitorear y evaluar (ME). A continuación se describirán los hallazgos encontrados en la Cooperativa del Magisterio de Túquerres – Coacremat

ME1Monitorear y Evaluar el Desempeño de TI: Los hallazgos o no conformidades encontradas se muestran en así:

Tabla 22: Hallazgo 1 ACMT

	**HALLAZGO COOPERATIVA DEL MAGISTERIO DE TÚQUERRES - COACREMAT**	**REF** **CH1-ME1**

PROCESO AUDITADO	Ambiente Físico		**PÁGINA** 1 DE 1	
RESPONSABLE	José Alexander Melo I			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Monitorear y Evaluar (ME)	**PROCESO**	Monitorear y Evaluar el Desempeño de TI (ME1)	

HALAZGO:

- No Existe un software para monitorear el rendimiento del sistema linix
- No se hacen reportes de monitoreo del sistema linix
- No se sacan estadísticas de los monitoreos a linix
- A partir de los monitoreos y las estadísticas no se realizan acciones correctivas a linix.

REF_PT: CD AUDITORIA DE SISTEMAS COACREMAT/CUESTIONARIO/ CUESTIONARIO_20

CONSECUENCIAS:

- Al no existir un software o proceso donde se haga un monitoreo al sistema linix, no se evaluaría su trabajo y los errores que se estén cometiendo.
- Al no hacer reportes de su evaluación no se corregiría posibles amenazas dentro de linix

- Al no hacer unas estadísticas para evaluar el funcionamiento no se tendría conocimiento de su funcionamiento.

RIESGO:

Probabilidad de ocurrencia:= 79%

Impacto según relevancia del proceso: Alto

RECOMENDACIONES:

- Implementar políticas para evaluación del sistema linix.
- Realizar un plan donde se monitoree al sistema linix para así sacar características que permitan ser evaluadas para tomar decisiones acertadas, esto se lo puede hacer con ayuda del fabricante del sistema linix.

5. INFORME DE AUDITORIA

Objetivo:

Realizar auditoria de sistemas a la Cooperativa del Magisterio de Túquerres – Coacremat para evidenciar las vulnerabilidades en la seguridad física, lógica, infraestructura tecnológica y software con el propósito de identificar y comprobar posibles amenazas a la que puede ser expuesta la información.

Objetivos específicos:

- Evaluar las políticas y los procedimientos para la evaluación de riesgos
- Establecer el estado de las políticas y los procedimientos en caminados a asegurar y garantizar la continuidad de los servicios de las tecnologías de la información.
- Evaluar las instalaciones en cuanto a la seguridad física
- Aportar información que permita a Coacremat implementar las medidas necesarias, para garantizar que los procesos realizados por sus usuarios tengan como materia prima información confiable, integra y confidencial, que asegure la trasparencia en los procesos.
- Evaluar el estado de la plataforma tecnológica que permita determinar las garantías que ofrece para la protección de datos.
- Analizar las políticas de seguridad existentes que garanticen la seguridad física y lógica de la información.

Limitaciones: La auditoría se realizó en completa normalidad, y se contó con la colaboración y acompañamiento de los funcionarios además se resalta que el sistema de información está en continua renovación y se han implementado nuevas características que benefician a la empresa.

Resultados de la auditoría: A continuación se presentan los resultados de la auditoría aplicada el sistema de información de la Cooperativa del Magisterio de Túquerres – Coacremat, presentando las recomendaciones de mejoramiento para cada uno de los procesos Cobit auditados.

DOMINIO - PLANIFICACION Y ORGANIZACIÓN (PO)

- **Proceso Cobit Po2: definir la arquitectura de la información**

Hallazgo

- En la Cooperativa del Magisterio de Túquerres – Coacremat no existe un procedimiento o software encargado de analizar los datos u archivos que se procesan en el sistema de información, estos datos fácilmente se pueden replicar en diferentes terminales, teniendo datos redundantes dentro de la Coacremat.
- No existe un software, diccionario de datos y esquema de clasificación de datos para eliminar datos redundantes que saturan al sistema de información puede que se eliminen datos que sean necesarios y se tengan datos almacenados que sean obsoletos dentro de los terminales de la empresa generando gasto en el espacio digital y volviendo al sistema redundante y lento.
- No existe un procedimiento o proceso de recuperación de archivos en línea ya que no se tiene unas políticas claras con respecto a este proceso, además Coacremat utiliza el internet como un medio de comunicación con las demás dependencias y sedes en diferentes partes del departamento de Nariño.

  REF CH1-PO2 (Tabla 6)

Recomendaciones

- Realizar seguimientos a los datos que se tienen dentro del sistema de información, teniendo un diccionario de datos y un esquema de clasificación de los mismos que sean propios de Coacremat.

- Implementar una política de reconocimiento de datos donde una persona sea la encargada de realizar la organización de datos para que sean organizados a través de un diccionario de datos y un esquema de clasificación de datos.

- Debe existir en todo el sistema procedimientos uniformes de validación para los datos ya que con esta validación se miraría los datos que son iguales y que se encuentran en dos o más lugares dentro del sistema de información para no generar duplicado de información es decir que la misma información sea más de una vez en un dispositivo de almacenamiento.
- Utilizar programas de recuperación de datos en línea

- Implementar un proceso de recuperación de datos y documentarlo para tener orden dentro de este procedimiento y para hacer las respectivas consultas cuando suceda algo parecido.

➢ **Proceso COBIT PO3: determinar la dirección tecnológica**

Hallazgo

- No existe políticas de evaluación de desempeño y calidad dentro de Coacremat, para medir la eficacia de los procesos que utilizan la plataforma tecnológica, evaluando los objetivos ejecutados y realizados identificando posibles anomalías y puntos críticos dentro del sistema de información y periódico donde se estimar cuantitativa y cualitativamente el grado de eficacia y eficiencia de cada uno de los procesos.

REF CH2 – PO3 (Tabla 7)

Recomendaciones

- Realizar procesos y políticas de autoevaluación de desempeño y calidad al sistema de información en su plataforma tecnológica.

- Aplicar estándares de desempeño y calidad dentro de la autoevaluación haciendo un modelado del sistema de información aplicando diferentes pruebas y sus consecuencias.

➢ **Proceso COBIT PO4: definir los procesos, organización y relaciones de TI**

Hallazgo

- No se cuenta con una persona encargada de la seguridad en el edificio.

- Dentro de las políticas de seguridad no se considera el servicio de celaduría para evitar posibles desmandes por parte de actores armados.
- No existe un control de las personas que acceden al departamento de sistemas que es de donde se maneja el sistema de información linix.

- Cualquier persona puede ingresar sin una credencial o permiso por parte de la cooperativa.

REF CH3 – PO4 (Tabla 8)

Recomendaciones

- Tener una política de seguridad física para la empresa que ejerza el control, inspección y vigilancia sobre de la cooperativa.

- Realizar un estudio sobre lo necesario de que una empresa de seguridad se encargue de adoptar las buenas normas de seguridad dentro de Coacremat.

- Realizar simulacros de infiltración de ladrones para mirar las vulnerabilidades de la empresa y que lugares son más seguros dentro de ella.

- Investigar al personal encargado de la seguridad.

- Realizar un servicio de identificación en la puerta

- Adoptar políticas de seguridad para la implementación de procesos de seguridad que beneficien a la empresa y que siempre se encuentren disponibles.

➢ **Proceso COBIT PO9: Evaluar y administrar los riesgos de TI**

Hallazgo

- Coacremat no cuenta con planes de contingencia antes riesgos potenciales que se pueden dar sin previo aviso.
- No existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo.
- No se registra el acceso al cuarto de servidores de personas ajenas a la dirección de sistemas
- No existe alarma para detectar condiciones anormales del ambiente en el cuarto del servidor.

REF CH1-PO9 (Tabla 9)

Recomendaciones

- Implementar políticas desde la gerencia para realizar un plan de amenazas que Coacremat puede tener, debe ser documentado para utilizarlo posteriormente donde se encuentren la amenaza que tipo de daño le haría a la empresa y el impacto a los procesos de la cooperativa.

- Elaborar el plan de contingencia que permita conocer puntos críticos en la empresa para garantizar un buen funcionamiento de la misma, logrando prevenir las incidencias antes de que estas ocurran.

- Elaborar e implementar un plan de mantenimiento de conservación como correctivo y preventivo que traten de ajustarse a la empresa para lograr un funcionamiento eficaz para obtener mejores resultado y no tener contratiempos en los procesos de Coacremat, también implantar un plan de mantenimiento de actualización para las aplicaciones o programas que lo requieran sin interferir en las configuraciones de los diferentes dispositivos.

- Elaborar una política de seguridad para el cuarto de servidores para mejorar la protección a saboteos y robo de dispositivos o de información.

- Realizar un estudio para implementar y mejorar el cuarto de servidores para que tenga las normas técnicas para alojar dichas maquinas.

DOMINIO ADQUIRIR E IMPLEMENTAR (AL)

- **Proceso COBIT AI2: Adquirir y mantener software aplicativo**

Hallazgo

- No existe un plan de gestión de riesgos de seguridad de las aplicaciones aprobado por la dirección
- No se han desarrollado aplicaciones para complementar el software empresarial

- La empresa no cuenta con un plan de aseguramiento de calidad de software

- La empresa no cuenta con una estrategia y un plan de mantenimiento de software

REF CH1-AL2 (Tabla 10)

Recomendaciones

- Implementar políticas desde la gerencia para la gestión de riesgos para el software ya que se debe interactuar con estos programas que deben ser probados antes de ser implantados en la plataforma tecnológica así

contribuyendo a mejorar la calidad del software y la satisfacción del cliente, volviendo los sistemas más confiables para el usuario final.

- Implementar políticas de desarrollo de software empresarial desde el departamento de sistemas que ayude a soportar algunos procesos y sea de ayuda y se integre con el sistema linix.

- Implementar un plan de aseguramiento de calidad de software donde se realicen pruebas como de sistemas, integración y aceptación del software que se desea ejecutar para disminuir problemas de incompatibilidad de software que potencialmente pueden perjudicar la información de la empresa.

- Implementar unas políticas donde se implementen programas y estrategias de planes de mantenimiento.

➢ **Proceso COBIT AI3: Adquirir y mantener infraestructura tecnológica**

Hallazgo

- No se tienen repuestos importantes, y actualizan este stock, en almacén.

- No se tienen planes con los equipos que han terminado su ciclo de vida.

REF CH2 –AL3(Tabla 11)

Recomendaciones

- Implementar un almacén donde se encuentren dispositivos de alta necesidad para la infraestructura tecnológica para garantizar un adecuado remplazo y así no generar una parálisis en os procesos.

- Implementar políticas de basura electrónica con equipos desactualizados donde se pueden incorporar a ciertas áreas y tomar las medidas adecuadas para que esos aparatos electrónicos sean desechados de manera correcta.

➢ **Proceso Cobit AL4: Facilitar la operación y el uso**

Hallazgo

- No se ha creado un documento donde se pueda identificar los aspectos técnicos, la capacidad de operación y los niveles de servicio de os diferentes programas que se encuentra usando la empresa.

REF CH3 – AL4(Tabla 12)

Recomendaciones

- Implementar un manual de usuario para las personas que manipulan los diferentes programas de la cooperativa donde se encontraría el uso de los programas y la solución de problemas que puedan suceder en la operación logrando disminuir los errores humanos que son unas de las principales causas para que el trabajo no sea óptimo.

➢ **Proceso Cobit AL6: Administrar cambios**

Hallazgos

- No se cuenta con un sistema o proceso que realice seguimiento y reporte a las solicitudes de cambio en el sistema de información.

REF CH4 – AL6(Tabla 13)

RECOMENDACIONES:

- Implementar políticas para contar con un sistema de gestión de solicitudes de cambio, esto se lo puede hacer a través de un desarrollo de software para la cooperativa.

Dominio Entregar y dar Soporte (DS)

➢ **Proceso Cobit DS3: Administrar el desempeño y la capacidad**

Hallazgo

- No se evalúa el desempeño y la capacidad del sistema de información linix.

- No existe un software o un mecanismo estadístico, que pueda dar respuesta, al desempeño actual en los procesos del sistema en toda la organización.

- No existen reuniones semanales o quincenales, por el departamento de sistemas para evaluar, los incidentes y procesos, en los cuales están a cargo.

- No se tiene respaldo de información en un servidor espejo.

REF CH1 – DS3(Tabla 14)

Recomendaciones

- Elaborar e implementar unas políticas de evaluación de la capacidad del sistema linix donde le proveedor puede colaborar a través de sus registros y al final se consolidaría la información para tener una autoevaluación de los procesos que maneja el sistema linix.

- Implementar un procedimiento o programa que gestione los datos de las evaluaciones para sacar estadísticas que servirán en un futuro ya que ellas muestran los posibles errores que pueden suceder a futuro.

- Implementar un cronograma de reuniones ya sean semanales o mensuales para verificar los datos de las evaluaciones de rendimiento de los procesos que tiene a cargo el sistema de información.

- Implementar un programa para encontrar respuesta a esta situación, no solo puede ser un servidor espejo, se puede guardar datos en la nube o albergar los backaps en otro lugar diferente a la sede central.

➢ **Proceso Cobit DS4: Garantizar la continuidad del servicio**

Hallazgo

- No se llevan a cabo pruebas de los procedimientos de recuperación de datos.

- No existen procedimientos para asegurar que las copias están adecuadamente protegidas y solo disponibles para el personal especialmente autorizado

- Actualmente la organización no posee alguna alternativa que permita la continuidad del desarrollo de los procesos normales, luego de una falla total en el sistema principal.

- No existe un repositorio de información sobre desastres ocurridos anteriormente que provean un panorama para posibles errores a futuro.

- No se lleva a cabo dentro de la organización algún tipo de registro sobre los errores más comunes, que permita un análisis de probabilidad de ocurrencia de fallas.

- Las personas que trabajan en la cooperativa no conocen los planes de continuidad para que el sistema trabaje de forma óptima.

REF CH2 – DS4(Tabla 15)

Recomendaciones

- Establecer un cronograma de pruebas de recuperación de datos donde se simule una situación donde implique utilizar este proceso de recuperación de datos.

- Implementar unas políticas de seguridad para salvaguardar las diferentes copias de seguridad existentes en la cooperativa del magisterio de Túquerres para que estas puedan ser utilizadas en una catástrofe que pueda ocurrir dentro de la cooperativa.

- Implementar un manual donde se encuentre que hacer después de una falla total del sistema de información que sirva de guía para futuras consultas.

- Elaborar un repositorio documentado de desastres ocurridos en la cooperativa donde se registren los problemas más comunes, ya que este será una guía para problemas que se pueden repetir en un futuro.

- Elaborar un manual para las personas que desconozcan los planes de continuidad del sistema de información o cualquiera de sus componentes para que sea utilizados los planes de contingencia de una forma correcta y no caer en errores humanos.

➢ **Proceso Cobit DS5: Garantizar la seguridad de los sistemas**

Hallazgo

- No se tiene planes de seguridad de TI implementados en la empresa.

- No se tienen identificado los riesgos que pueden interferir en el sistema de información.

- No se cuenta con un documento o plan de seguridad dentro de la cooperativa.

- Las copias de seguridad de los datos no cuentan con claves de acceso

REF CH3 – DS5(Tabla 16)

Recomendaciones

- Implementar políticas gerenciales para construir un plan de seguridad informática que satisfaga las necesidades de los sistemas de información de Coacremat así como cada uno de los componentes que son parte de este para qué se pauten las actividades relacionadas con la seguridad informática.

- Al implementar las políticas de seguridad informática elaborar un documento con los puntos críticos del sistema de información, identificando posibles vulnerabilidades en el sistema.
- Colocar clave a las copias de seguridad para que proteja la integridad de los datos que se encuentran en estos dispositivos.

➢ **Proceso Cobit DS8: Administrar la mesa de servicio y los incidentes**

Hallazgo

- En la empresa no se registra los diferentes incidentes que se pueden presentar.
- No se llevan registros de las consultas realizadas por los usuarios (registro y rastreo de llamadas, incidentes, solicitudes de servicio y necesidades de información).

REF CH4 – DS8(Tabla 17)

Recomendaciones

- Elaborar e implementar políticas y procesos donde se registren los incidentes informáticos de los diferentes componentes de los sistemas de información para obtener unos datos y hacer un seguimiento para mejorar el servicio.

- Implementar políticas de registros de incidentes, elaborando un manual donde el usuario pueda participar de los diferentes incidentes que le suceda en el sistema de información.

➢ **Proceso Cobit DS9: Administrar la configuración**

Hallazgo

- No existe un responsable encargado de la gestión de la configuración de los diferentes terminales.

- No existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo.

- La cooperativa no tiene un plan de mantenimiento y configuración de los dispositivos, y no está documentado.

REF CH5 – DS9(Tabla 18)

Recomendaciones

- Implementar un manual de funciones donde se encuentren las tareas bien definidas con su perfil profesional par que cada persona realice las tareas asignadas.

- Implementar un mantenimiento preventivo cada mes para prevenir posibles errores cuando el sistema esté en producción.

- Realizar planes de mantenimiento a todo el sistema de información con documentación para lograr una mejor optimización de los dispositivos que conforman el sistema.

➢ **Proceso Cobit DS10: Administración de problemas**

Hallazgo

- Los problemas que se reportan no son categorizados.

- Los problemas no son documentados para tener un registro y posteriormente utilizarlos para resolver un incidente.

REF CH6-DS10(Tabla 19)

Recomendaciones

- Implementar un documento donde se reporten las diferentes incidencias del sistema de información para categorizarlos y analizar sus resultados para tomar decisiones con respecto al problema que se haya encontrado.

- Implementar políticas gerenciales que ayuden a tomar decisiones con respecto al os problemas que suceden en el sistema de información.

➢ **Proceso Cobit: Administración de datos**

Hallazgo

- No verifican que las copias de seguridad sean iguales, ósea que la integridad de los datos iguales a las originales.

- No se tienen procedimientos que permitan la reconstrucción de un archivo digital, el cual fue inadvertidamente destruido.

- No existe un control estricto de las copias de seguridad.

REF CH6-DS11(Tabla 20)

Recomendaciones

- Implementar una verificación de datos en las copias de seguridad para verificar posibles alteraciones a esta información.

- Implementar un software que permita recuperar un archivo en caso de que este se haya borrado de forma accidental.

- Implementar un controla las copias de seguridad para que estas sean utilizadas exclusivamente por personal autorizado.

➢ **Proceso Cobit DS12: Administración del ambiente físico**

Hallazgo

- No existen una persona responsable de la seguridad
- No existe personal de vigilancia en la institución
- No existe vigilancia en el cuarto del servidor

- Se permite el acceso a los archivos y programas al personal de la cooperativa sin importar su rol
- No se ha instruido al personal sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización
- No existen extintores de fuego
- Los interruptores de energía no están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos
- No existe salida de emergencia

REF CH – DS12(Tabla 21)

Recomendaciones

- Implementar políticas de seguridad física que comprometa a la gerencia para contrata una persona idónea y con responsabilidad para la vigilancia del edificio.

- Implantar un sistema de monitoreo para el cuarto del servidor, pueden ser cámaras o sensores de movimientos que informen al encargado de este lugar que existen personas no autorizadas manipulando el cuarto de servidores.

- Utilizar un programa o crear roles de usuarios donde no se permita ver archivos de otras personas y tener cuidado con los comandos que permiten mirar archivos en cualquier parte del sistema de información, estos no deben ser suministrados a ninguna persona.

- Implementar simulacros donde puedan verificar el estado psicológico de cada persona para afrontar posible amenazas como la entrada de personas que tengan intenciones de robar, para que así el personal este más atento y maneje un proceso que se ira creando según la necesidad de la cooperativa.
- Adquirir extintores de fuego para neutralizar posibles incendios, estos deben estar a la mano y muy cerca de puntos que sean posibles focos de incendios.

- Etiquetar los interruptores de energía para saber que voltaje tienen y tratar de que estos no sean obstaculizados por objetos que no dejen mirar que tipo de conector es.

- Implementar una salida de emergencia para que permita una rápida evacuación del edificio en caso de catástrofes naturales.

Dominio Monitorear y evaluar (ME)

- **Proceso Cobit ME1: Monitorear y Evaluar el Desempeño de TI**

Hallazgo

- No Existe un software para monitorear el rendimiento del sistema linix
- No se hacen reportes de monitoreo del sistema linix
- No se sacan estadísticas de los monitoreos a linix
- A partir de los monitoreos y las estadísticas no se realizan acciones correctivas a linix.

REF CH1 – ME1(Tabla 22)

Recomendaciones

- Implementar políticas para evaluación del sistema linix.

- Realizar un plan donde se monitoree al sistema linix para así sacar características que permitan ser evaluadas para tomar decisiones acertadas, esto se lo puede hacer con ayuda del fabricante del sistema linix.

6. INFORME GERENCIAL

DOCTOR:

Mario Fernando Rodríguez Chávez

Gerente de la cooperativa del magisterio de Túquerres

Atento saludo

Luego de realizarlos procesos correspondientes a la auditoria del sistema de información de Coacremat de la sede principal en Túquerres, se observó lo siguiente:

Los resultados de la auditoria serán resumidos por cada uno de los cuatro dominios de COBIT (Objetivos de Control para Información y Tecnologías Relacionadas).

- **DOMINIO - PLANIFICACION Y ORGANIZACIÓN (PO)**

Los procedimientos o procesos que se tienen en el sistema de información generan archivos que se vuelven redundantes y obsoletos ya que a la vez se generan actualizaciones a estos en alguna parte del sistema de información.

Para esto se debe realizar un seguimiento a los archivos que se generan después de un proceso y tener en cuenta las propiedades de los mismos para no generar manipulación de información.

Se debe implementar políticas de evaluación de desempeño y calidad del sistema de información y no solo del sistema linix, ya que con este tipo de análisis se puede identificar posibles anomalías y puntos críticos dentro del sistema reduciendo la calidad del procesamiento de los datos.

Falta diseñar planes de contingencia ante riesgos potenciales al sistema de información ya que pueden legar sin previo aviso y pueden generar perdida de información relevante de información de Coacremat.

Teniendo los puntos críticos después de un análisis se debe realizar dicho plan de contingencia que abarque el funcionamiento del sistema de información en su totalidad.

Es notable el uso de las tics en Coacremat ya que a través de estas se encuentran oportunidades tecnológicas según los requerimientos de la cooperativa donde la base de datos es uno de los fuertes tecnológicos integrando diversidad de datos y procesamiento de los mismos.

- **DOMINIO –ADQUIRIR E IMPLEMENTAR (AL)**

Se debe tener en cuenta un plan de riesgos para la seguridad de las aplicaciones que se integran con el sistema de información, para lograr mayor seguridad teniendo en cuenta los riesgos las probabilidades de impacto y las consecuencias que se pueden generar a través de estos problemas.

Se debe realizar un plan de mantenimiento con un manual e historial de los diferentes mantenimientos que ha tenido un dispositivo ya que sirve como historial y se puede resolver problemas recurrentes con solo lee el historial del mantenimiento.

En caso de emergencia se debe suplir al departamento de sistemas con repuestos de los diferentes dispositivos que integran el sistema de información para una rápida solución de problemas o hacer un convenio de repuestos de entrega inmediata teniendo en cuenta que tipo de dispositivo y que parte es la que se afectó.

Es importante realizar planes con los equipos que terminan el ciclo de vida en Coacremat para no tener un cumulo de basura electrónica dentro de las instalaciones ya que por causas naturales pueden oxidarse y desprender olores que pueden generar enfermedades a las personas que laboran en el edificio.

Aunque no existe un sistema de gestión de solicitudes o un proceso que defina una solicitud de cambio es importante implementar ya que se tiene mayor información y organización del hardware o software que se ha cambiado en el sistema de información, esto se lo puede hacer a través de un desarrollo de software interno de la Coacremat.

Se destaca el fortalecimiento de las tecnologías de la información y comunicación que hace Coacremat con el cambio de la plataforma tecnológica que hizo recientemente y software como linix que ayuda a la gestión de información de la cooperativa para una mejor atención a sus asociados.

- **DOMINIO – ENTREGAR Y DAR SOPORTE(DS)**

En cuanto a la evaluación del desempeño del sistema linix y la capacidad, debe ser evaluada por Coacremat para generar reportes de calidad a la empresa que se ha contratado ejecutora y desarrolladora del sistema linix.

Como se maneja información importante se debe tener un servidor espejo que entre en funcionamiento inmediatamente después de una anomalía en la sede principal de Coacremat y no dejar que se retrasen los procesos que se pueden ejecutar normalmente.

Se debe implementar una estrategia de incidentes que se pueden generar en la empresa para prestar una mejor calidad en el servicio que los usuarios externos e internos.

Los planes de mantenimiento a las terminales deben estar documentados en lo posible tener formatos donde se haga un historial de cada equipo o dispositivo con hora de mantenimiento que tipo de mantenimiento se hizo para no generar conflictos y revisiones recurrentes a cada computador.

Se debe verificar, analizar y categorizar los problemas que se generen en el sistema de información de Coacremat implementando una documentación donde se reporten las incidencias y el impacto que estas puedan crear.

Se debe implementar un sistema de monitoreo para el servidor principal como cámaras o sensores que se encarguen de dar aviso sobre el ambiente y de las personas que ingresan de forma ilegal a este recinto.

Las empresas contratantes con los diferentes componentes del sistema de información que tiene la cooperativa Coacremat dan soporte eficaz donde se hace una actualización constante de conocimientos a las personas que utilizan dichos componentes.

- **DOMINIO – MONITOREAR Y EVALUAR (ME)**

Se recomienda tener un software para monitorear el rendimiento del sistema linix donde se realicen reportes y se saquen estadísticas para que a partir de estos monitoreos se visualicen los posibles problemas y se realicen acciones correctivas.

Se destaca la eficacia de los funcionarios del área de sistemas ya que constantemente quieren conocer la evolución de los procesos que se realizan en la empresa para lograr una mayor confiabilidad y servicio hacia los asociados.

7. CONCLUSIONES

Coacremat como una empresa innovadora en las tecnologías quiere estar a la vanguardia de estas para prestar un mejor servicio a sus asociados es por eso que se hace una auditoria para analizar y evaluar el sistema de información para encontrar posibles falencias y soluciones a estas.

Por medio de las diferentes técnicas de auditoria, en este caso el Cobit se hace un análisis detallado al sistema de información, su seguridad, la parte física, lógica y humanos que conlleva a fraudes, es ahí donde toma importancia la seguridad informática y como se debe hacer una auditoria para que la información este bien resguardada.

La información es uno de los activos más importantes en las empresas de hoy en día es por ello que se deben hacer supervisiones continuas a los sistemas de información para generar confianza a los usuarios.

La evaluación y análisis del Cobit con respecto a la auditoria de sistemas que se hizo en Coacremat muestra las diferentes falencias que existe dentro del entorno digital y como suplir estas necesidades a través de planes de contingencia.

La auditoría de sistemas es una herramienta que garantiza que un sistema funcione de manera adecuada, siempre y cuando se hagan los correctivos necesarios.

8. RECOMENDACIONES

Realizar seguimientos a los datos que se tienen dentro del sistema de información, teniendo un diccionario de datos y un esquema de clasificación de los mismos que sean de Coacremat.

Adoptar políticas de seguridad para la implementación de procesos de seguridad que beneficien a la empresa y que siempre se encuentren disponibles.

Elaborar una política de seguridad para el cuarto de servidores para mejorar la protección a saboteos y robo de dispositivos o de información.

Implementar un plan de aseguramiento de calidad de software donde se realicen pruebas como de sistemas, integración y aceptación del software que se desea ejecutar para disminuir problemas de incompatibilidad de software que potencialmente pueden perjudicar la información de la empresa.

Implementar políticas de desarrollo de software empresarial desde el departamento de sistemas que ayude a soportar algunos procesos y sea de ayuda y se integre con el sistema linix.

Implementar un manual de usuario para las personas que manipulan los diferentes programas de la cooperativa donde se encontraría el uso de los programas y la solución de problemas que puedan suceder en la operación logrando disminuir los errores humanos que son unas de las principales causas para que el trabajo no sea óptimo.

Implementar políticas para contar con un sistema de gestión de solicitudes de cambio, esto se lo puede hacer a través de un desarrollo de software para la cooperativa.

Implementar un cronograma de reuniones ya sean semanales o mensuales para verificar los datos de las evaluaciones de rendimiento de los procesos que tiene a cargo el sistema de información.

Implementar simulacros donde puedan verificar el estado psicológico de cada persona para afrontar posible amenazas como la entrada de personas que tengan intenciones de robar, para que así el personal este más atento y maneje un proceso que se ira creando según la necesidad de la cooperativa.

REFERENCIAS BIBLIOGRÁFICAS

ECHENIQUE GARCIA, José A., Auditoría en informática, 2ª Ed., Mc GRAW-HILL, México D.F., 2005.

http://bibdigital.epn.edu.ec/handle/15000/1019

http://es.scribd.com/doc/21156297/16/PLAN-DE-SEGURIDAD-INFORMATICA

http://portal.aerocivil.gov.co/portal/page/portal/Aerocivil_Portal_Intranet/seguridad_informatica/mejore_seguridad_informacion/incidentes/incidente_seguridad_informatica

http://www.gerencie.com/auditoria-de-sistemas-de-informacion.html

http://www.isaca.org/knowledge-center/cobit/Pages/Overview.aspx

http://www.monografias.com/trabajos14/auditoriasistemas/auditoriasistemas.shtml

http://www.monografias.com/trabajos93/cobit-objetivo-contro-tecnologia-informacion-y-relacionadas/cobit-objetivo-contro-tecnologia-informacion-y-relacionadas.shtml

http://www.slideshare.net/arelyochoa/auditoria-de-sistema-etapas

ISACA, COBIT 4.1 Castellano (En línea). En: ISACA Colombia (Bogotá). Disponible en la dirección electrónica: http://www.isaca-bogota.net/metodologias/cobit.aspx 281

PIATTINI Mario, DEL PESO Emilio, Auditoría en informática: un enfoque práctico, 2ª Ed., Alfaomega/RA-MA, México D.F., 2001

PINILLA F. José D., Auditoría informática: un enfoque operacional, ECOE, Bogotá, 1995

SOLARTE, Francisco Nicolás, GUSTÍN Enith, HERNANDEZ Ricardo. Manual De Procedimientos para Llevar a la Práctica La Auditoría Informática y de Sistemas, IUCESMAG, Pasto, 2013.

ANEXOS

Nota: Los anexos se entregan en medio digital y constan de:

- Cuadro de definición de fuentes de conocimiento:

  Se encuentran en la carpeta FUENTE _DE_CONOCIMIENTO_CDFC consta de archivos llamados CDFC y van desde CDFC1 hasta CDFC4.

- Evidencias

  Fotográficas:

  Se encuentra una carpeta llamada PRUEBAS consta de archivos llamados AUDC y van des AUDC_1 hasta AUDC_68

  Evidencias de audio:

  Se encuentra una carpeta llamada PRUEBAS consta de archivos llamados AAC y van desde AAC1 hasta AAC79

- Cuestionarios:

  Se encuentra una carpeta llamada CUESTIONARIOS consta de archivos llamados CUESTIONARIO_ y van desde CUESTIONARIO_1 hasta CUESTIONARIO_20 donde se encuentran las preguntas y a la vez sus evidencias.