INDICE

CAPITULO I

INTRODUCCION

ANTECEDENTES

La Armada del Ecuador es una institución que forma parte de las Fuerzas Armadas Ecuatorianas, cuya finalidad es preservar la integridad territorial y soberanía nacional, misión que lo logra a través de sus miembros tanto militares como civiles.

La Fuerza Armada surge con la Independencia del dominio español y constituida la Gran Colombia. La creación de la Primera Escuela Náutica para formación de Oficiales fue el 9 de Octubre de 1822, la misma que se lo hace mediante Decreto.

Durante el año 1952 se crean las zonas navales, la Aviación Naval y la Infantería de Marina. Además se ve la necesidad de preparar Oficiales y personal de Tripulantes miembros que serían indispensables para el cumplimiento de sus objetivos, por esta razón se crea la Escuela de Especialidades de Tripulantes en el año de 1955.

Así mismo, para implementar la capacidad técnica y profesional del personal, modernizó sus establecimientos educacionales, como la Academia de Guerra Naval, la Escuela Naval que toma la categoría de Instituto Superior, el Centro de Instrucción Naval, la Escuela de la Marina Mercante, el Agrupamiento de Apoyo del Cuerpo de Infantería de Marina y la Escuela de Aviación.

De esta manera al aumentar la capacidad y responsabilidad impartida a esta Fuerza por el Gobierno Nacional, se ve la necesidad de incluir dentro de sus miembros a personal civil, quienes no solo contribuirán al cumplimiento de sus objetivos, sino que ayudarían al desarrollo profesional, técnico y administrativo.

Estructura Organizacional de la Armada del Ecuador

La Armada del Ecuador se caracteriza por tener una estructura totalmente lineal, esto se da por cuanto forman parte de las Fuerzas Armadas, por lo tanto, es necesario regirse por Leyes y Reglamentos impartidos desde su organismo central, este es el Ministerio de Defensa Nacional.

Direcciones y sus funciones principales

Comandancia General de la Marina.

Es el Órgano a través del cual el Comandante General de Marina ejerce el Comando y la Administración de la Armada.

Órganos de Asesoramiento

Consejos Varios: La función básica es la de asesorar al Comandante General de Marina en los asuntos previstos en la Ley Orgánica de las Fuerzas Armadas y otros por determinar.

Órganos de Planeamiento y Control

Empresas de la Armada: Dentro de éstas tenemos a Transportes Navieros Ecuatorianos, Flota Petrolera Ecuatoriana, Astilleros Navales Ecuatorianos, KAMAROS S.A. Centro de Investigaciones fomento y explotación de recursos bioacuáticos.

Estado Mayor de la Armada: Asesorar al Comandante General de Marina en el ejercicio del Comando Superior de la Armada. Es el Órgano de Planeamiento para el alistamiento y empleo del Poder Naval.

Inspectoría General de la Armada: Controla las actividades operativas, administrativas y financieras de la Institución.

Dirección de Inteligencia Naval: Su función es producir inteligencia y difundirla a los Repartos de la Armada y al Comando Conjunto.

Direcciones Operativas

Comando de Operaciones Navales: Su función básica es preparar, administrar y conducir las Fuerzas Operativas en la realización de Operaciones Militares.

Órganos de Línea Técnico Administrativas

Secretaría General de la Armada: Es la encargada de planificar, organizar, ejecutar y controlar los procedimientos de normalización administrativa y la sistematización de los servicios administrativos de carácter general, a nivel Armada. Coordina y apoya las actividades y el asesoramiento al Comandante General de Marina.

Dirección General del Personal: Tiene la función de administrar los recursos humanos de la Armada.

Dirección General de Educación: Formar, especializar y perfeccionar profesionalmente a los miembros de la Institución.

Dirección General de Finanzas: Administra los recursos económicos y patrimonio de la Armada.

Dirección General del Material: Planifica, organiza y ejecuta la logística de producción, administra los recursos materiales y proporciona el apoyo logístico en su sector, que sean requeridos por los Repartos Navales.

Dirección General de Intereses Marítimos: Planifica, organiza, dirige y controla la participación de la Armada en el fortalecimiento del Poder Marítimo Nacional, excepto el factor relacionado con el Poder Naval.

Dirección de la Marina Mercante: Administra las actividades relacionadas con la Marina Mercante Nacional, el transporte por agua y su infraestructura portuaria, ejerce el control de las actividades ilícitas y garantiza la vida en el mar.

Dirección informática (DINFOR)

La Dirección de informática (DINFOR) fue creada para coordinar, ejecutar, y supervisar las políticas, normas y planes de sistematización de la base administrativa de la Armada. De igual forma esta dirección era la encargada de armonizar las acciones de implantación y desarrollo informático en la institución y para conseguirlo debía existir una adecuada comunicación con los Centros de Procesamientos de datos (CEPROD), a fin de que, los objetivos institucionales sobre esta materia, se cumplan.

Los CEPROD era la unidad técnica de la DINFOR.

La Dirección de informática de la Armada, conciente de la necesidad de lograr un alto grado de modernización y equipamiento en el sector informático, requiere de políticas y objetivos que permitan normar, estandarizar y optimizar el desarrollo informático de la

institución. Por dicha razón el Comando General decide emitir, en el año de 1997, las " Guías de Informática " que en este campo se requieren, a fin de que a través de éstas, se plasme técnicamente el procesos de la información en forma efectiva y eficiente, con el apoyo de recursos para el Procesamiento Automático de datos.

Centro de Procesamiento de datos (CEPROD)

Eran los centros ejecutores de proyectos informáticos de la Armada, además daban asesoramiento de índole técnico a la centros de computo y a la DINFOR. Existía un CEPROD para toda la Armada por lo que sus tareas no eran realizadas con la suficiente eficiencia y eficacia que se deseaba.

Éstos centros trimestralmente debían entregar un informe pormenorizado de las actividades cumplidas durante cada período; avance y situación de los proyectos de acuerdo al Plan de sistematización del Reparto, precisando los sistemas que se encuentran en desarrollo y explotación, además lo que estaba previsto conseguir y lo que se alcanzo en realidad.

Guías Informáticas

Las guías fueron creadas para orientar a dar principios de aplicación general de carácter obligatorio para los Centros de Procesamientos de Datos en cada unos de los Repartos de la Armada. Estas guías deben ser revisadas y actualizadas a fin de que se adapten a la política y requerimientos informáticos de la Institución debido a que la tecnología cambia constantemente. También es importante conocer que estas guías se

tenían que retroalimentar por medio de las sugerencias de los repartos que interactuaban con ellas.

Estas guías están dividas en volúmenes, cada uno de los cuales cubre aspectos de carácter general, sobre temas específicos. A continuación se presenta los volúmenes y una breve descripción de los mismos.

VOLUMEN I POLÍTICAS DE INFORMÁTICA

Tienen como propósito dar a conocer las políticas de carácter general que tiendan a que la gestión del área de informática de los Repartos de la Armada, se desarrollen bajo un marco de normatividad, especialmente en lo que se relaciona con el desarrollo de las actividades y a la utilización de los recursos que intervienen en los diferentes procesos en el ámbito informático, con miras a coadyuvar en el cumplimiento de los objetivos institucionales.

VOLUMEN II GUÍAS PARA LA ADMINISTRACIÓN DE LOS CEPROD

Tienen como propósito dar lineamientos de carácter general que propendan a que la coordinación de la Dirección de Informática con los Centros de Procesamiento de Datos de los distintos Repartos sea eficiente.

VOLUMEN III GUÍAS PARA PLANIFICAR LA GESTIÓN INFORMÁTICA

Tiene como propósito, establecer lineamientos de carácter general con el objeto de que la planificación de proyectos informáticos se desarrolle bajo normas y métodos de trabajo con el fin de aprovechar eficientemente los recursos, apoyar en la forma de decisiones, evaluar alternativas, desarrollar proyectos informáticos, realizar provisiones y controlar la gestión de los resultados.

VOLUMEN IV CONTROLES Y SEGURIDADES EN LOS CENTROS DE COMPUTO

Tienen como propósito dar a conocer en forma general los controles y seguridades que obligatoriamente deben observarse en los Repartos, a fin de salvaguardar la información calificada, equipos computacionales y demás recursos informáticos de los Centros de Procesamiento de Datos de la Armada.

VOLUMEN V GUÍAS SOBRE DESARROLLO DE PROYECTOS INFORMÁTICOS

Tienen como propósito establecer conceptos y directrices estándares que se deben utilizar en las diferentes etapas del ciclo de vida de un proyecto informático.

VOLUMEN VI GUÍAS DE PROGRAMACIÓN

Tienen como propósito, establecer lineamientos de carácter general, que propendan a lograr uniformidad en el estilo y calidad del diseño, la codificación y documentación de programas.

VOLUMEN VII GUÍAS SOBRE ESTÁNDARES DE DOCUMENTACIÓN

Tienen como propósito, indicar los estándares que determinan la forma en que la documentación ha de prepararse y mantenerse, de modo que se pueda transmitir información de analistas, programadores, operadores, ejecutivos y usuarios.

Sin embargo estas guías no fueron conocidas por todo el personal, en especial, por aquellos miembros recién ingresados a la Armada, consecuentemente, estas guías no fueron utilizadas por todos los repartos trayendo con esto que no se apliquen las guías y

que el proceso de actualización continúa de las guías no se cumpla. Actualmente las Guías no tienen vigencia alguna.

SITUACION ACTUAL

Debido a la naturaleza de las instituciones públicas de adaptarse a las políticas de estado y a sus necesidades, la Armada se vio en la necesidad de cambiar su estructura organizacional para adaptarse a las nuevas necesidades de control y de funciones.

Por dicha razón la naturaleza DINFOR para la cual fue creada quedo obsoleta entonces la Armada sustituyo la DINFOR por La Dirección de Desarrollo Administrativo e Informático (DIRDAI).

La Dirección de Desarrollo Administrativo e Informático es una unidad técnico administrativa subordinada al Estado Mayor de la Armada y su misión es implementar una base administrativa que permita optimizar la estructura organizacional, funcional y normativa, así como la automatización de los sistemas administrativos a través del desarrollo y utilización de la tecnología informática y de comunicaciones.

Y su función básica es:

Planificar, desarrollar, normalizar y mantener la base administrativa de la Armada, así como la sistematización y automatización de los sistemas y procedimientos administrativos que permitan racionalizar y facilitar el reordenamiento de la gestión administrativa, a través de la implementación de la tecnología informática y de comunicaciones, considerando las políticas del mando y el Plan Estratégico Institucional.

La DIRDAI esta compuesta por dos departamentos que son:

- Dirección de desarrollo administrativo.
- Dirección de desarrollo informático.

Cada departamento tiene la función de:

- Planificar, implementar y ejecutar la normalización y desarrollo de la base administrativa de acuerdo al Plan Estratégico Institucional, a fin de optimizar y racionalizar los sistemas, normas y procedimientos administrativos de la Armada. En el caso de la dirección de desarrollo administrativo.

- Planificar, desarrollar, implantar, ejecutar y evaluar el Plan Informático Institucional, así como proponer a través de estudios de factibilidad la automatización de los procesos administrativos en los Repartos Navales, y dirigir la aplicación y utilización de la tecnología informática y de comunicaciones, en base a las políticas y programas de la Armada. En el caso de la dirección de desarrollo informático.

Al tener esta nueva estructura organizacional con funciones y tareas claramente definidas se pensaría en una mejor solución a las necesidades de la Armada, sin embargo, esto no se cumple principalmente debido a la falta de personal en los dos departamentos mencionados anteriormente. Esto trae consigo que muchas de las funciones que se deben cumplir por parte del departamento de dirección informática no se realicen o se delegan a otros departamentos como el CETEIN (Centro de Tecnología de información).

Otro inconveniente que se nota es que la burocracia no permite agilitar ciertos trámites que permitirían un mejor desempeño de la DIRDAI – DIN.

Actualmente existe muy poco control, por parte de la Armada, para el ámbito informático y los procesos que interactúan con el. Por ejemplo no se aplican estándares en el área de desarrollo de software, se cumplen parcialmente los estándares en redes, entre otras.

La Armada cuenta con el departamento de auditorías pero la misma no tiene en su estructura organizacional una división que haga mención a la auditoria informática.

JUSTIFICACIÓN

La inversión que cada institución realiza para la automatización de sus procesos y el mantenimiento de los mismos tienen que estar debidamente respaldada y justificada, más aún cuando se trata de una institución militar y pública como lo es la Armada, ya que está expuesta a un permanente control por parte de las autoridades gubernamentales.

En instituciones militares como la Armada, en donde el uso óptimo de los recursos es una Política de Estado, se debe implantar normas rigurosas que permitan mantener un adecuado control de las actividades que se realizan y de esta manera poder establecer las anomalías existentes y sus autores. Estos controles se los debe realizar de una manera continua además que deben estar documentados para conocer los temas que abarcan, los parámetros a tomar en cuenta, los medios para obtener la información, los formatos existentes para realizar reportes, entre otras.

A pesar de que la Auditoría Informática es una disciplina cuya práctica es poco realizada en nuestro país, la misma, es importante en las organizaciones por las siguientes razones:

- Evitar la difusión y utilización de resultados o información errónea esto se produce cuando la calidad de datos de entrada es inexacta o los mismos son manipulados, lo cual abre la posibilidad de que se provoque un efecto dominó y afecte seriamente las operaciones, toma de decisiones e imagen de la empresa.
- Que las computadoras, servidores y los Centros de Procesamiento de Datos se han convertido en blancos apetecibles para fraudes, espionaje, delincuencia y terrorismo informático.
- Que la continuidad de las operaciones, la administración y organización de la empresa no deben descansar en sistemas mal diseñados, ya que los mismos pueden convertirse en un serio peligro para la empresa.
- Que las bases de datos pueden ser propensas a atentados y accesos de usuarios no autorizados o intrusos.
- Que la vigencia de la Ley de Derecho de Autor, la piratería de software y el uso no autorizado de programas, con las implicaciones legales y respectivas sanciones que esto puede tener para la empresa.
- Que el robo de secretos comerciales, información financiera, administrativa, la transferencia ilícita de tecnología y demás delitos informáticos.
- Que la insatisfacción de los usuarios debido a que no reciben el soporte técnico adecuado o no se reparan los daños de hardware ni se resuelven los problemas en plazos razonables, es decir, el usuario percibe que está abandonado y desatendido permanentemente.

- El incremento desmesurado de costos del departamento de Sistemas.
- Un nivel bajo de riesgos en lo que respecta a seguridad lógica, seguridad física y confidencialidad.
- El mantener la continuidad del servicio y la elaboración y actualización de los planes de contingencia para lograr este objetivo.
- El uso inadecuado de la computadora para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor y el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

Debido a que la Armada del Ecuador es una Institución Pública, se debe tener muy en cuenta las Leyes que rigen en cuanto al manejo de Empresas Públicas del Estado, estas leyes se encuentran dictadas por la Contraloría General del Estado, por lo tanto, este Manual deberá tener bases legales que constan en la Ley Orgánica de la Contraloría General del Estado, debido a que la Contraloría aún no cuenta con normas específicas para la realización de Auditorías Informáticas, se toman algunos artículos.

(LOAFYC Art. 257)"La auditoría gubernamental consiste en un examen objetivo, sistemático y profesional de las operaciones financieras y profesional de las operaciones financieras o administrativas, o de ambas a la vez, practicado con posterioridad a su ejecución, con la finalidad de verificarlas, evaluarlas y elaborar el correspondiente informe que debe contener comentarios, conclusiones y recomendaciones y, en caso de examen de los estados financieros, el respectivo dictamen profesional.".

(Art. 258) “La auditoría gubernamental comprende las siguientes actividades:

- Verificar las transacciones, registros, informes y estados financieros correspondientes al período examinado.
- Determinar el cumplimiento de las disposiciones legales y reglamentarias, políticas y demás normas aplicables.
- Revisar y evaluar el control interno financiero.
- Examinar y evaluar la planificación, organización, dirección y control interno administrativo.
- Revisar y evaluar la eficiencia, efectividad y economía con que se han utilizado los recursos humanos, materiales y financieros.
- Revisar y evaluar los resultados de las operaciones programadas, a fin de determinar si se han alcanzado las metas propuestas.”

El pleno conocimiento de todas las actividades, que están relacionadas de manera directa o indirecta con el ámbito informático, es primordial para conocer el grado de eficiencia y eficacia en el que se encuentran y de esta manera tomar medidas necesarias; esta es la razón es por la que se debe implantar un manual de procedimientos.

El Manual de Procedimientos de Auditoría permitirá contar con un documento en el que exista puntos y objetivos de control, basados en estándares internacionales, que ayude a la Armada a evaluar el ámbito informático y los procesos que interactúan con el.

El contar con un Manual de Procedimientos de Auditoría Informática, permitirá a la Armada minimizar e identificar el riesgo de filtración y mal manejo de información, así como también el uso incorrecto de los recursos asignados a cada reparto para la ejecución de sus proyectos.

ALCANCE

El manual de procedimientos para auditoría informática, pretende reemplazar a las guías informáticas existentes desde el año de 1997. El alcance estará determinado por los procedimientos dados en el manual para realizar una auditoría informática en las siguientes áreas:

- PETI (Plan Estratégico de Tecnologías de Información).
- Estructura Organizacional.
- Seguridades.
- Redes y Comunicaciones.
- Desarrollo de Proyectos Informáticos.
- Software en Explotación.

Los procedimientos de auditoría para las áreas antes mencionadas, se encuentra detallados en el Capítulo 4, el alcance de las auditorías dependerá de la experiencia del Auditor, así de hasta donde se pretenden controlar los procedimientos existentes.

OBJETIVOS

Objetivo General

- Realizar un Manual de procedimientos de Auditoría Informática para la Armada del Ecuador.

Objetivos Específicos

- Investigar una metodología para desarrollar el Manual de Procedimientos de Auditoría.
- Levantar los procesos informáticos existentes actualmente en la Dirección de Desarrollo Informático (DIRDAI-DIN).
- Adaptar el Análisis de Riesgos para establecer las áreas críticas que interactúan con el ambiente informático.
- Establecer los puntos y objetivos de control que permitan realizar un análisis de las diferentes áreas que interactúan con el ámbito informático de la Armada.

CAPITULO II

MARCO TEÓRICO

INTRODUCCIÓN

La palabra auditoría proviene del latín "**auditorius"** que significa la persona que tiene la virtud de oír y revisar cuentas. En cada área donde se aplica la palabra auditoría ésta permite evaluar procesos, procedimientos y tareas enmarcado en un objetivo especifico.

En informática se evalúa la eficiencia y eficacia con que los procesos informáticos funcionan para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

La Auditoría Informática, entonces, 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.

Mediante la Auditoría Informática o de Sistemas se verifica la existencia y aplicación de todas las normas y procedimientos requeridos para minimizar las posibles causas de riesgos tanto en las instalaciones y equipos, como en lo programas computacionales y los datos, en todo el ámbito del Centro de Cómputos: usuarios, instalaciones, equipos.

Las Instituciones realizan Auditorías, con la finalidad de asegurar la eficiencia de las organizaciones de informática, así como la confiabilidad y seguridad de sus sistemas. Finalmente la Auditoría Informática es de vital importancia para el buen desempeño de los

sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad.

Objetivos Generales de una Auditoría informática

- Asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles.
- Conocer la situación actual del área informática y las actividades y esfuerzos necesarios para lograr los objetivos propuestos.
- Apoyo de función informática a las metas y objetivos de la organización.
- Capacitar y educar sobre controles en las Tecnologías de Información

Controles

Conjunto de disposiciones metódicas, cuyo fin es vigilar las funciones y actitudes de las empresas y para ello permite verificar si todo se realiza conforme a los programas adoptados, ordenes impartidas y principios admitidos.

Clasificación general de los controles

1. **Controles Preventivos**

Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones .

2. **Controles detectivos**

Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. Son los mas importantes para el auditor. En cierta forma sirven para evaluar la eficiencia de los controles preventivos.

3. Controles Correctivos

Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en si una actividad altamente propensa a errores.

Principales Controles físicos y lógicos

Controles particulares tanto en la parte física como en la lógica se detallan a continuación:

- **Autenticidad**

  Permiten verificar la identidad de los passwords y firmas digitales.

- **Exactitud**

  Aseguran la coherencia de los datos.

- **Totalidad**

  Evitan la omisión de registros así como garantizan la conclusión de un proceso de envío.

- **Redundancia**

  Evitan la duplicidad de datos.

- **Privacidad**

  Aseguran la protección de los datos.

- **Existencia**

  Aseguran la disponibilidad de los datos.

- **Protección de Activos**

  Destrucción o corrupción de información o del hardware.

- **Efectividad**

  Aseguran el logro de los objetivos.

- **Eficiencia**

  Aseguran el uso óptimo de los recursos.

Tendencias en Tecnología de Información

Cuando se habla de tendencias, se habla de dirección, y de la posibilidad de que en un futuro, ciertas tecnologías que todavía no tienen nombre y apellido, alcancen la madurez como para ser comercialmente viables y que puedan insertarse en el mercado.

Pero cuando se habla de tecnología de información, se entra en un territorio de fronteras cada vez más amplias, difusas, y de cambios cada vez mas frecuentes, debido a que la tecnología es cambiante.

El futuro ambiente tecnológico, deberá considerar la adopción de modelos de negocio centrados en la Web, que utilizan herramientas y estándares de Internet, y garantizan la omnipresencia de los servicios y la información, organizándose con una arquitectura de tres niveles claramente separados: la interfase al usuario, la lógica de negocios y la gerencia transaccional de las bases de datos.

El ciclo de vida de la tecnología y la estrategia de adquisición e implantación se convierten en factores críticos de la adopción racional y efectiva de tecnología. Esto se refleja en conceptos tales como el Costo Total de Propiedad, como criterio orientador de las decisiones de compra, y el Ciclo de Implantación de Tecnología, el cual debe considerar al año Web como valor de referencia, entre otros.

Los gobiernos y las empresas privadas deben pensar cada vez más y con más frecuencia en la tecnología de información como fuente de valor; lo físico y lo virtual

deben coexistir y complementarse, versus la superposición actual que en forma implacable castiga al físico y premia al virtual.

Tendencias organizacionales

Hay que transitar el camino basada en una tendencia organizacional con un marcado culto al papel y al acopio de información y dirigirse hacia una basada en la productividad colectiva, el trabajo colaborativo y la confianza, más la adopción simbiótica de sistemas de información digitalizados.

En esta nueva tendencia se premia y aprecia la capacidad de: distribución de información, trabajar en equipo e interactuar sobre los sistemas a distancia.

La tendencia antigua de creer que el personal se percibe solo como ”usuario” de los sistemas, va desapareciendo y surge una nueva tendencia en el que los usuarios son “contribuyentes” o “prestadores de servicios” que aportan información y conocimientos al sistema, conscientes de que su calidad y forma son importantes para ser usados efectivamente por el resto de la comunidad.

El adiestramiento ya no sólo debe orientarse a tecnificar o impartir destrezas específicas en el manejo de las aplicaciones y los sistemas, sino que debe centrarse en crear un nuevo tipo de trabajador del conocimiento, que parte de valores que determinan su comportamiento y percepción de su rol/función dentro de la cadena de aporte de valor. Este planteamiento se basa en generar un movimiento asociado a la implantación de los cambios en materia de tecnología de información, que traiga como consecuencia una transformación de la cultura y la forma como ésta es manejada; para lo cual es necesario basarse en tres elementos fundamentales:

- Educación para partir de procesos formales de transferencia de tecnología y de inducción para adopción de nuevas tendencias.
- Confianza para proveer a los usuarios de los sistemas de un ambiente que permita eliminar las barreras que obligan a las personas a adueñarse de la información.
- Políticas y directrices basadas en una visión global y compartida.

Curva de Madurez Tecnológica

Toda tecnología tiene su ciclo de vida, es decir, comienza como una investigación que va tomando forma conforme ésta sea útil y aceptada por las empresas que se dedican al desarrollo tecnológico, llegando a su punto pico cuando las necesidades inicialmente propuestas han sido cubiertas casi en su totalidad, declinando conforme aparecen nuevos requerimientos tecnológicos, esto trae consigo el surgimiento de nuevas tecnologías que seguirán cubriendo estos requerimientos y así sucesivamente. En el siguiente gráfico se puede observar el ciclo de vida de la tecnología.

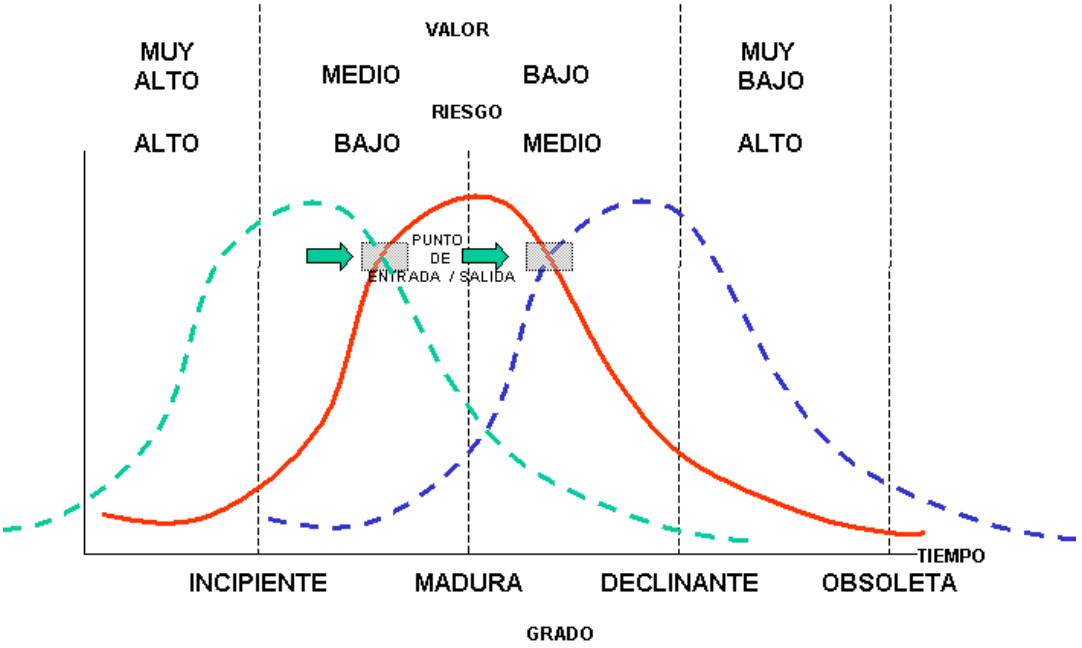


Figura 2.1 (Curva de Madurez Tecnológica)

Transición tecnológica

Para manejar la transición hacia el nuevo ambiente tecnológico se sugiere:

- Revisar el modelo de negocios en función de las reglas definidas y analizar constantemente las necesidades de información acorde al entorno.
- Definir una visión tecnológica que responda a las funciones o procesos organizacionales y no a la estructura organizativa, pues si esta cambia, la visión tecnológica perdería vigencia o ameritaría ser revisada.
- Considerar a la gente como parte de cualquier estrategia de actualización tecnológica, ayudándolos a adquirir las capacidades para comprender, asimilar y adoptar las nuevas facilidades de transformación.
- Evaluar la conveniencia del modelo de contratación delegada a terceros en el análisis de costos y seguridad.
- Simplificar y unificar la diversidad de plataformas y ambientes de desarrollo, así como consolidar las bases de datos.

- Identificar oportunidades de racionalización y reorganización apoyadas en la tendencia convergente de tecnologías de datos, voz y vídeo.
- Utilizar aceleradores que permitan portar las aplicaciones existentes al nuevo ambiente, minimizando esfuerzos y dedicándolos a satisfacer requerimientos nuevos que no se hayan atendido o que se vayan a presentar en el futuro inmediato.
- Extender el uso de la tecnología SAN (Storage Area Network) para el manejo de archivos, revisar los mecanismos de almacenamiento secundario y la evaluación profunda de las estrategias de Data Warehousing.
- Adoptar servicios de respaldo remoto, contingencia de datos y aplicaciones, virtualización y otras estrategias habilitadas por la tecnología.

Productividad de proyectos de tecnología de información

En las últimas décadas se ha pretendido mejorar la productividad en el desarrollo de proyectos de tecnología de información y la calidad del mismo mediante la aplicación de nuevas metodologías y tecnologías; sin embargo, las organizaciones se han dado cuenta que el problema fundamental radica en su incapacidad para gestionar el proceso del desarrollo. Con el uso de métodos y técnicas mejores no se consiguen los beneficios esperados si los procesos se caracterizan por la indisciplina y el desorden. Por tanto, se hace necesario establecer un plan de acción para medir y mejorar la calidad del proyecto de desarrollo; es decir, que lo transforme en un proceso capaz de entregar los productos a tiempo, gestionando su comportamiento a través de las fases del proyecto y teniendo en cuenta la percepción de la Calidad del Cliente. Este plan de acción se implementa a través de métodos cuyo objetivo es evaluar el proceso de los proyectos de tecnología de las organizaciones y mejorar su capacidad.

La medición de los proyectos de tecnología de información y su importancia

Existen 4 razones por las cuales se miden los procesos, productos y recursos:

- Para entender los procesos, productos, recursos y el entorno o ambiente con el objetivo de establecer las bases de comparación con futuras evaluaciones.
- Para evaluar, es decir, determinando la situación actual con respecto a los planes, lo que permite saber cuando los proyectos y procesos pueden estar desviándose con la idea de poderlos mantener bajo control, verificar si se han alcanzado las metas de calidad establecidas y conocer el impacto que pueden tener los cambios sobre los productos y procesos.
- Para predecir, con la idea de poder planear y entender la relación entre los procesos y productos y la construcción de modelos basados en los atributos que puedan ser usados para establecer metas de costo, tiempo y calidad, extrapolando tendencias y proyecciones basados en datos históricos que además ayuden a analizar riesgos.
- Para mejorar, con el objetivo de obtener información que ayude a identificar la causa raíz de los problemas, ineficiencias y otras oportunidades para mejorar la calidad del producto y el desempeño de los procesos.

Todas las iniciativas de medición dentro de los Proyectos de Tecnología de Información están basadas en las razones anteriormente expuestas, sin embargo, normalmente se encuentra con un alto nivel de dificultad en cómo cuantificar el efecto de dichas iniciativas, lo cual solo es posible a través del uso de Métricas.

Métricas

Las métricas son los datos cuantificables que permiten caracterizar a los procesos y productos de Tecnología de Información, de la misma manera como se caracterizan los objetos físicos en términos de longitud, altura y profundidad.

El primer nivel de métricas consiste en 7 categorías básicas llamadas Métricas Primitivas; el resultado de las distintas combinaciones entre estas métricas se denomina Métricas Computadas o Combinadas.

Métricas Primitivas

En el caso de los proyectos de tecnología, para efectos de su efectiva planeación y control, se consideran 11 métricas primitivas, incluyéndose en la lista: Gastos, Progreso, Trabajo Completado y Asuntos Pendientes.

- Tamaño. El tamaño es la medida más crítica de los proyectos de tecnología asociado a sistemas de información. Cuando se puede estimar el tamaño del producto, se puede reducir el riesgo del proyecto y del cliente. El tamaño del sistema podrá directamente impactar las otras métricas y es un componente clave de productividad, desempeño y capacidad. Existen tres métodos generalmente aceptados para determinar el tamaño de un sistema: Puntos de Función, Líneas de Código y Páginas de Documentación.
- Esfuerzo. Esta métrica mide el número de horas laborables realmente gastadas para completar una tarea. El esfuerzo es relevante cuando se determina la cantidad de personal requerido para un proyecto.

- Duración. Mide el número de días calendarios requeridos para desarrollar una tarea o completar un proyecto.
- Defectos. Provee una visión de la calidad y confiabilidad de los productos entregados a los clientes y de los procesos que se usan para generar dichos productos. Esta métrica mide los defectos en dos maneras: Faltas y Fallas. Las faltas son incluidas y detectadas en el ciclo de vida del sistema y son los defectos desde el punto de vista de los desarrolladores. Las fallas son manifestaciones de faltas detectadas durante la operación del sistema; las fallas representan los defectos desde el punto de vista de los usuarios.
- Personal. Esta métrica provee el número de personas asignadas al proyecto. Permite determinar exactamente el número de personal que ha trabajado en el proyecto.
- Recursos de Computación. Esta métrica determina cuántos recursos de computación han sido usados durante el proyecto, facilitando las futuras estimaciones al basarse en estos números.
- Cambio. Esta métrica establece el número de cambios hechos a los requerimientos del proyecto durante su desarrollo; ayudan a determinar el impacto del cambio y la forma como se maneja en la organización.
- Gastos. Costo del proyecto total, en términos de recursos humanos y materiales adquiridos y gastados en su desarrollo.
- Progreso. Progreso estimado en comparación con el progreso actual.
- Trabajo Completado. Total del proyecto que ha sido completado con relación al alcance, evaluado en términos de trabajo realizado, tareas, actividades y fases.
- Asuntos Pendientes. Número de preguntas que no pueden ser inmediatamente resueltas por el equipo del proyecto y que requieren un compromiso para buscar su

solución o que pueda requerir una decisión de alguien externo al equipo del proyecto.

Para que la comparación de las métricas primitivas sea válida entre proyectos de tecnología, es importante considerar el ambiente en el cual se desarrollará el mismo, es decir, se deben examinar la plataforma del Hardware, Software, Lenguajes de Programación y Ambiente de Desarrollo sobre el cual se está operando ya que esto puede afectar el significado de los que se puede obtener en las métricas.

Métricas Computadas o Combinadas

En términos de prioridad, todos los proyectos deberían mantener y reportar como mínimo las métricas de Duración, Esfuerzo y Trabajo Completado. La necesidad de otras métricas debe ser determinada de acuerdo al nivel de riesgo del proyecto y el nivel de preparación de la organización para obtener otras métricas.

La combinación de dos o más métricas primitivas representa una valiosa información gerencial. Cuando se utilizan métricas computadas, no solo se puede medir el estado actual de proceso y del producto en un tiempo dado, sino que también, a lo largo del tiempo, ayuda a determinar si el proceso está mejorando y si los productos se entregan con la calidad y confiabilidad que el cliente espera del proyecto.

El verdadero conocimiento surge de este tipo de métrica y a su vez es la base fundamental para la toma de decisiones. Es importante no enfocarse en una sola métrica, se debe evaluar todas en conjunto con el objetivo de visualizar claramente las debilidades y fortalezas del proyecto.

FUNCIÓN DE LA AUDITORÍA

La función auditora ***debe ser absolutamente independiente*** no tiene carácter ejecutivo, ni son vinculantes sus conclusiones. Queda a cargo de la Armada tomar las decisiones pertinentes. La auditoría contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones. Aunque pueden aparecer sugerencias y planes de acción para eliminar las disfunciones y debilidades antedichas; estas sugerencias plasmadas en el Informe final reciben el nombre de Recomendaciones.

La auditoría informática puede ser de dos tipos que son: la auditoría interna y la externa

Auditoría Informática Interna: Es la realizada con recursos materiales y personas que pertenecen a la Armada. Los empleados que realizan esta tarea son remunerados económicamente. La auditoría interna existe por expresa decisión de la Armada, o sea, que puede optar por su disolución en cualquier momento.

Auditoría Informática Externa: Es realizada por personas u empresas externas a la Armada y presupone una mayor objetividad que la Auditoría Interna, debido al mayor distanciamiento entre auditores y auditados.

La auditoría informática interna cuenta con algunas ventajas adicionales muy importantes respecto de la auditoría externa, por ejemplo, la auditoría interna tiene la ventaja de que puede actuar periódicamente realizando Revisiones globales, como parte de su Plan Anual y de su actividad normal. Los auditados conocen estos planes y se habitúan a las Auditorías, especialmente cuando las consecuencias de las Recomendaciones habidas benefician su trabajo.

ALCANCE

El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoría informática, se complementa con los objetivos de ésta. El alcance ha de figurar expresamente en el plan de auditoría, de modo que quede perfectamente determinado no solamente hasta que puntos se va a llegar, sino áreas serán omitidas. Ejemplo: No se analizará la metodología utilizada para el desarrollo de software.

La indefinición de los alcances de la auditoría compromete el éxito de la misma.

OBJETIVO

Analizar las T.I. cuando estén operativos para evaluar la eficiencia y eficacia de los mismos. Este objetivo debe conseguirse tanto a nivel global como parcial.

NECESIDAD DE AUDITORIA INFORMÁTICA

Se acude a las auditorías informáticas cuando existen síntomas bien perceptibles de debilidad en cualquiera de las siguientes áreas:

- P.E.T.I.
- Estructura Organizacional.
- Software en explotación.
- Software en desarrollo.
- Comunicaciones y redes.
- Seguridades.

Estos síntomas pueden agruparse en clases:

- Síntomas de descoordinación y desorganización:
    - No coinciden los objetivos de la Informática de la Compañía y de la propia Compañía.

- Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente. (Puede ocurrir con algún cambio masivo de personal, o en una reestructuración fallida de alguna área o en la modificación de alguna Norma importante)

- Síntomas de mala imagen e insatisfacción de los usuarios:

  - No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de Software en los terminales de usuario, refrescamiento de paneles, variación de los ficheros que deben ponerse diariamente a su disposición, etc.

  - No se reparan las averías de Hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.

- No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de Aplicaciones críticas y sensibles.

- Síntomas de debilidades económico-financiero:

  - Incremento desmesurado de costos.

  - Necesidad de justificación de Inversiones Informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).

  - Desviaciones Presupuestarias significativas.

  - Costos y plazos de nuevos proyectos.

- Síntomas de Inseguridad: Evaluación de nivel de riesgos

  - Seguridad Lógica

  - Seguridad Física

- Confidencialidad

- Continuidad del Servicio. Es un concepto aún más importante que la Seguridad.

- Centro de Proceso de Datos fuera de control. Si tal situación llegara a percibirse, sería prácticamente inútil la auditoría. Esa es la razón por la cual, en este caso, el síntoma debe ser sustituido por el mínimo indicio.

Los datos son propiedad inicialmente de la organización que los genera.

HERRAMIENTAS

Las herramientas para realizar un proceso de auditoría informática son las siguientes:

- Cuestionario (Check list).
- Estándares. (Software, hardware, etc.)
- Simuladores (Generadores de datos, prototipos, etc.).
- Paquetes de auditoría.
- Matrices de riesgo. (CRAMM)
- Formatos de presentación de informes

PERFIL DEL AUDITOR INFORMÁTICO

La persona que realice auditoria informática debe ser Ingeniero en sistemas con experiencia en:

- Desarrollo y explotación de Proyectos informáticos en software y / o hardware.
- Conocer las metodologías de desarrollo de software.

- Conocimientos en redes y comunicaciones.
- Conocer metodologías de auditoría informática.

FUNCIONES

Las funciones de análisis y revisión que el auditor informático realiza, puede chocar con la psicología del auditado, ya que es un informático y tiene la necesidad de realizar sus tareas con racionalidad y eficiencia. La reticencia del auditado es comprensible y, en ocasiones, fundada. El nivel técnico del auditor es a veces insuficiente, dada la gran complejidad de los Sistemas, unidos a los plazos demasiado breves de los que suelen disponer para realizar su tarea.

Además del chequeo de los Sistemas, el auditor somete al auditado a una serie de cuestionario. Dichos cuestionarios, llamados Check List[1], deben ser guardados celosamente por la Armada, ya que son activos importantes de su actividad.

Los Check List tienen que ser comprendidos por el auditor al pie de la letra, ya que si son mal aplicados y mal recitados se pueden llegar a obtener resultados distintos ocasionando prejuiciosos ya que los Check List puede llegar a explicar cómo ocurren los hechos pero no por qué ocurren.

El auditor sólo puede emitir un juicio global o parcial basado en hechos y situaciones incontrovertibles, careciendo de poder para modificar la situación analizada por él mismo.

[1] **Check List:** Se refiere a las listas de verificación con las que trabaja el auditor

METODOLOGÍAS DE AUDITORIA INFORMÁTICA

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

Para dar una clasificación de las auditorias informáticas diremos que son de dos tipos:

- Generales.
- Especificas.

Metodologías Generales

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

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

Metodologías Específicas

Las metodologías especificas son aquellas que el auditor interno o externo “crea” para su uso son mas especificas y exhaustivas, ya que sirve para evaluar un área en particular, al igual que la anterior metodología sus informes permiten el registro de observaciones.

Tanto las metodologías generales como especificas tienen un pequeño inconveniente y es que tienden a depender mucho de la experiencia de los profesionales que las usan o

crean ya que éstas pertenecen al tipo de metodologías denominadas “Cualitativas” las cuales se basan en el criterio y raciocinio humano capaz de definir un proceso de trabajo, en base a la experiencia acumulada. .

Cabe anotar que las metodologías de análisis de riesgos no se usa para auditoria informática aunque es un muy buen ejemplo de lo que seria una metodología denominada “cuantitativas”.

Como se menciono anteriormente las metodologías para auditoria informática son parecidas mas no iguales, ya que poseen en general casi las mismas fases para un proceso de auditoria informática, por dicha razón, se ha decidido analizar las siguientes metodologías en donde se explicará las fases.

Metodología para el desarrollo e implantación de la auditoria en informática propuesta por ENRIQUE HERNANDEZ HERNANDEZ

Hernández recomienda que la auditoría en informática debe respaldarse por un proceso formal que asegure su previo entendimiento por cada unos de los responsables de llevar a la practica dicho proceso en la empresa. Además sugiere que no es recomendable fomentar la dependencia, en el desempeño de esta función, en la experiencia, habilidades, criterios y conocimientos del auditor sino que debe existir una referencia metodológica.

La función de auditoría informática debe contar con un desarrollo de actividades basado en un método de trabajo formal, que sea entendido por las personas que van a ser auditoría y debe ser complementado con técnicas y herramientas propias de la función.

Es importante señalar que el uso de cualquier metodología de auditoria informática no garantiza por sí sola el éxito de los diferentes planes de A.I[2]. se requiere también de un buen dominio y uso constante de los siguientes aspectos complementarios:

- Técnicas.
- Herramientas de productividad.
- Habilidades personales.
- Conocimientos técnicos y administrativos.
- Experiencia en los campos de auditoría en informática.
- Conocimiento de los factores del negocio y del medio externo al mismo.
- Actualización permanente.
- Involucramiento y comunicación constante con asociaciones nacionales e internacionales relacionadas con el campo.

Metodología

Hernández propone de 6 etapas que son:

1. Preliminar - Diagnóstico
2. Justificación.
3. Adecuación.
4. Formalización.
5. Desarrollo.
6. Implantación.

[2] A.I. Auditoria Informática.

1. **Etapa preliminar o diagnostico de la situación actual.**

Esta etapa pretende conocer las opiniones de la alta dirección par estimar el grado de satisfacción y confianza que tiene en los productos, servicios y recursos de informática; así mismo, detecta la fortalezas, aciertos y apoyo que brinda dicha función desde la perspectiva de los directivos del negocio.

El estudio preliminar de la situación actual también involucra al aspecto informático para lo cual se coordina directamente con el responsable de la función informática y se toma en consideración los siguientes temas:

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

2. **Etapa de justificación.**

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

Los productos de etapa son:

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

3. **Etapa de adecuación.**

Esta etapa tiene como objetivo principal adaptar el proyecto a las características del negocio, sin olvidar la referencia de los estándares políticas y procedimientos de auditoría comúnmente aceptados y recomendados por las asociaciones relacionadas con el proceso, así como las formuladas y aprobadas de manera particular en los negocios para informática.

Al terminar la presente etapa, el auditor en informática contará con un proyecto bien especificado y clasificado; en las etapas restantes solo se desarrolla e implanta lo definido.

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

4. **Etapa de formalización.**

Esta etapa corresponde a la alta gerencia y consiste en aprobarla consecuentemente dar su apoyo para la realización de este proyecto de auditoría.

5. **Etapa de desarrollo.**

Al fin el auditor ejerce su función de manera practica. Esta fase comprende:

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

6. **Etapa de implantación.**

En esta fase el trabajo de auditoria ha concluido ya que el auditor entregó el informe, consecuentemente, el personal que esta involucrado con las áreas afectadas ejecuta las conclusiones y recomendaciones que se encuentran en el informe del auditor

Metodología para el proceso de Auditoria Informática. DR. WELLINGTON RIOS

Ríos propone 4 fases para un correcto proceso de auditoria éstos son:

1. Estudio preliminar.

2. Revisión y evaluación de controles y seguridades.
3. Examen detallado de áreas críticas.
4. Comunicación de resultados.

1. Estudio Preliminar.

Para Ríos esta fase es de vital importancia ya que los resultados de esta fase pueden con llevar a la suspensión de la auditoría si se considera y evidencia que no existen mayores problemas y justificativos en la aplicación de controles y seguridades; o por lo contrario constituye un valioso aporte para la planificación del examen.

Además en esta fase se realiza la compilación y análisis de documentos que contienen disposiciones generales, políticas y objetivos de la unidad, no se realiza lecturas de manuales, reglamentos, disposiciones legales, etc. Ya que pueden o no ser revisados en las siguientes fases, dependiendo si se consideran o no como áreas críticas.

Ríos recomienda la utilización de las siguientes técnicas de investigación para cumplir de mejor manera esta fase:

- Entrevistas
- Cuestionarios
- Observación directa
- Encuestas, etc.

2. Revisión y evaluación de controles y seguridades.

Ríos sugiere que en esta etapa se precise las áreas críticas que serán examinadas con profundidad en la siguiente fase, y a su vez elimina sistemas y procedimientos que no ameritan, bajo una relación costo - beneficio, invertir recursos para profundizar su examen.

En esta fase se cuenta con la participación directa del auditor de sistemas y no se requiere aun de especialistas. Además se sugiere el uso de las siguientes herramientas:

- listas de chequeo (cuestionario).
- Narrativas.
- Diagramas de flujo.

Además de otras técnicas, que permitan precisar las áreas críticas a las cuales debe orientar la auditoría propiamente, es decir, el ámbito del examen, los recursos necesarios y el tiempo que le consumirá la auditoría.

3. Examen detallado de áreas criticas.

Para Ríos esta es la fase más importante de la Auditoría Informática, ya que se requiere mayor tiempo que las dos anteriores, y según sea la complejidad, se requiere de especialistas en informática que sean el soporte de las actividades técnicas que haya que profundizar. El desarrollo de esta fase se la realiza exclusivamente en el campo, y es prácticamente la culminación del trabajo de auditoría.

Los procedimientos de esta fase se centran hacia la identificación de hallazgos que incluyen acciones correctivas que ameritan ser recomendadas en el informe, por tal motivo es aconsejable preparar no un programa sino tantos como áreas críticas se hayan

identificado en la fase anterior, de tal suerte que se facilite su ejecución por separado por parte del auditor o especialista según sea el caso.

Además Ríos da atributos para el registro de hallazgos que son:

- **CONDICION:** Situación encontrada: "Lo que es".
- **CRITERIO:** Medida, norma, ley aplicable: "Lo que debe ser".
- **CAUSA:** Motivos por los que se originó la desviación.
- **EFECTO:** Repercusión de las acciones deficientes (cuantificable).

4. Comunicación de resultados.

En base a los resultados obtenidos de la fase anterior, es decir de los hallazgos descritos en las hojas de apuntes, se procede a la elaboración del borrador del informe con la correspondiente aprobación de Auditoría Interna.

Metodología de Auditoría Informática. VARIOS AUTORES

Este proceso de auditoria informática pasa por las siguientes etapas:

1. Alcance y Objetivos de la Auditoría Informática.
2. Estudio inicial del entorno auditable.
3. Determinación de los recursos necesarios para realizar la auditoría.
4. Elaboración del plan y de los Programas de Trabajo.
5. Actividades propiamente dichas de la auditoría.
6. Confección y redacción del Informe Final.
7. Redacción de la Carta de Introducción o Carta de Presentación del Informe final.

1. Alcance y Objetivos de la Auditoría Informática

El alcance de la auditoría expresa los límites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias y las organizaciones a auditar. Es importante también determinar cuales materias, funciones u organizaciones no van a ser auditadas.

Las personas que realizan la auditoría han de conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar. Deben comprender los deseos y pretensiones del cliente, de forma que las metas fijadas puedan ser cumplidas.

Una vez definidos los objetivos (objetivos específicos), éstos se añadirán a los objetivos generales y comunes de a toda auditoría Informática: La operatividad de los Sistemas y los Controles Generales de Gestión Informática.

2. Estudio Inicial del entorno auditable

Para realizar dicho estudio ha de examinarse las funciones y actividades generales de la informática.

Para su realización el auditor debe conocer lo siguiente:

1. Organización
    - Organigrama.
    - Departamentos.
    - Relaciones Jerárquicas y funcionales entre órganos de la Organización.
    - Flujos de Información.

- Número de Puestos de trabajo.
- Número de personas por Puesto de Trabajo.

2. Entorno Operacional

El equipo de auditoría informática debe poseer una adecuada referencia del entorno en el que va a desenvolverse. Este conocimiento previo se logra determinando, fundamentalmente, los siguientes extremos:

- Situación geográfica de los Sistemas.
- Arquitectura y configuración de Hardware y Software.
- Inventario de Hardware y Software.
- Comunicación y Redes de Comunicación.

3. Aplicaciones bases de datos y ficheros

El estudio inicial que han de realizar los auditores se cierra y culmina con una idea general de los procesos informáticos realizados en la empresa auditada. Para ello deberán conocer lo siguiente:

- Volumen, antigüedad y complejidad de las Aplicaciones
- Metodología del Diseño
- Documentación
- Cantidad y complejidad de Bases de Datos y Ficheros.

3. Determinación de los recursos necesarios para realizar la auditoría

Mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría.

- Recursos materiales

    a. Recursos materiales Software

        Programas propios de la auditoria: Son muy potentes y Flexibles.

        Monitores: Se utilizan en función del grado de desarrollo observado en la actividad de Técnica de Sistemas del auditado y de la cantidad y calidad de los datos ya existentes.

    b. Recursos materiales

        Los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en las Computadoras del auditado. Para lo cuál habrá de convenir, tiempo de maquina, espacio de disco, impresoras ocupadas, etc.

- Recursos Humanos

La cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado depende de la materia auditable.

4. Elaboración del Plan y de los programas de trabajo

Una vez que se asignan los recursos, el responsable de la auditoría y sus colaboradores establecen un plan de trabajo. Decidido éste, se procede a la programación del mismo.

El plan se elabora teniendo en cuenta, entre otros criterios, los siguientes:

a) Si la Revisión debe realizarse por áreas generales o áreas específicas. En el primer caso, la elaboración es más compleja y costosa.

b) Si la auditoría es global, de toda la Informática, o parcial. El volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal.

- En el plan no se consideran calendarios, porque se manejan recursos genéricos y no específicos.
- En el Plan se establecen los recursos y esfuerzos globales que van a ser necesarios.
- En el Plan se establecen las prioridades de materias auditables, de acuerdo siempre con las prioridades del cliente.
- El Plan establece disponibilidad futura de los recursos durante la revisión.
- El Plan estructura las tareas a realizar por cada integrante del grupo.
- 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 plan debe ser lo suficientemente flexible como para permitir modificaciones a lo largo del proyecto.

5. Actividades propiamente dichas de la Auditoría

Si se realiza una auditoria por grandes áreas 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.

Para realizar el proceso de auditoria se emplean las siguientes técnicas de auditoría:

- Análisis de la información recabada del auditado.
- Análisis de la información propia.
- Cruzamiento de las informaciones anteriores.
- Entrevistas.
- Simulación.
- Muestreos.

Las siguientes herramientas.

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

Confección y redacción del Informe Final

La función de la auditoría se materializa exclusivamente por escrito. Por lo tanto la elaboración final es el exponente de su calidad. Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

CAPITULO III

LEVANTAMIENTO DE PROCESOS

INTRODUCCIÓN

El levantamiento de procesos que se realizó en la Armada del Ecuador se lo hizo tomando en cuenta el estándar utilizado en la mencionada institución. Dichos procesos toman en cuenta las tareas realizadas por la DIRDAI-DIN y el CETEIN.

Estos procesos no son más que las tareas que hasta ese momento se las venía realizando sin tener en cuenta los manuales que poseía la Armada sino que los realizaban por costumbre.

El levantamiento de los procesos se lo hizo con la supervisión de la DIRDAI –DAD entidad que en la Armada se encarga de realizar el levantamiento de todos los procesos que existen.

A continuación se presenta los procesos previamente aprobados por el mencionado departamento. (ANEXO 1)

CAPITULO IV

METODOLOGIA

METODOLOGIA DE AUDITORIA INFORMÁTICA

Este plan esta compuesto de 3 puntos:

1. Estudio preliminar.
2. Examen detallado de la áreas criticas.
3. Comunicación de resultados.

Estudio preliminar

Esta fase es de vital importancia ya que su estudio involucra al área de informática , por ser este un sector totalmente cambiante en su aplicación al ritmo que va evolucionando la técnica. Es importante mencionar que los resultados de esta fase pueden con llevar a la suspensión de la auditoria si el auditor considera y evidencia que no existen mayores problemas y justificativos en la aplicación de controles y seguridades; o por lo contrario constituye un valioso aporte para la planificación del examen.

Esta etapa es una de las más importantes del proceso debido a que se precisa áreas críticas que serán examinadas con profundidad en la siguiente fase, y a su vez elimina sistemas y procedimientos que no ameritan, bajo una relación costo-beneficio, invertir recursos para profundizar su examen.

Para esta fase se utilizara la metodología de CRAMM (Metodología de Análisis y Gestión de Riesgos) que se explica a continuación.

Finalmente producto de esta fase serán las áreas que serán auditadas y su alcance.

Metodología de CRAMM

La metodología CRAMM (Metodología de Análisis y Gestión de Riesgos) permite un análisis cualitativo y cuantitativo de la situación actual de la organización para lo cual se apoya en una matriz en donde las filas representan los diferentes "activos de información"[3] y las columnas los riesgos que amenazan la integridad, confidencialidad y disponibilidad de estos activos.

Es necesario que se conozca las definiciones de la integridad, confidencialidad y disponibilidad.

" **Integridad:** Se refiere a la precisión y suficiencia de la información así como su validez de acuerdo con los valores y expectativas.

Confidencialidad: Se refiere a la protección de información sensible contra la divulgación no autorizada.

Disponibilidad: Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso del negocio ahora y en el futuro. "[4]

La metodología para evaluar la integridad, confidencialidad y disponibilidad de los activos de información se basa en las siguientes tablas.

[3] **Activo de información:** Es la información que poseen los sistemas.
[4] Definiciones tomadas de la metodología de COBIT

Tabla de integridad y sus valores de impacto

El requerimiento de cumplimiento, precisión y resistencia a modificaciones no autorizadas. Cada custodio puede tener diferentes tipos de activos de información electrónica que necesita ser categorizada individualmente. En base a lo anterior, las categorías sugeridas para la integridad son las siguientes:

Tabla 2.1 (Tabla de integridad)

CATEGORÍA	VALOR	INFORMACION
REQUERIMIENTO BAJO	1 – 3	PARA SU MODIFICACIÓN SE NECESITA DE AUTORIZACIÓN DEL ÁREA.
REQUERIMIENTO MODERADO	4 – 7	PARA SU MODIFICACIÓN SE NECESITA DE AUTORIZACIÓN A NIVEL DEPARTAMENTAL.
REQUERIMIENTO ALTO	8 – 9	PARA SU MODIFICACIÓN SE NECESITA DE AUTORIZACIÓN A NIVEL ORGANIZACIONAL.
REQUERIMIENTO ABSOLUTO	10	PARA SU MODIFICACIÓN SE NECESITA DE AUTORIZACIÓN A NIVEL GUBERNAMENTAL.

Tabla de confidencialidad y sus valores de impacto

Se identifica el requerimiento de protección a fin de que no la conozcan personas no autorizadas para así mantener su confidencialidad. En base a lo anterior, las categorías sugeridas para la confidencialidad son las siguientes:

Tabla 2.2 (Tabla de confidencialidad)

CATEGORÍA	VALOR	INFORMACIÓN
CONFIDENCIAL	1 – 3	PEDIDO LEGITIMO
RESERVADA	4 – 5	SU PERDIDA, ALTERACIÓN O USO PUEDE OCASIONAR ALGÚN DAÑO AL GOBIERNO, A UNA AGENCIA, PERSONA U ORGANIZACIÓN
SECRETA	6 – 7	SU PERDIDA, ALTERACIÓN O USO PUEDE OCASIONAR DAÑO SUBSTANCIAL AL GOBIERNO, A UNA AGENCIA, PERSONA U ORGANIZACIÓN
SECRETÍSIMA	8 – 10	SU DIVULGACIÓN PUEDE LLEVAR A LA GUERRA

Tabla de disponibilidad y sus valores de impacto

La habilidad para recuperar la información, en el caso de interrupción, a fin de seguir apoyando los procesos de la organización:

Tabla 2.3 (Tabla de disponibilidad)

REQUERIMIENTO	VALOR	INFORMACIÓN
BAJO	1 - 3	SIGNIFICANDO QUE SI LA INFORMACIÓN NO ES DISPONIBLE TENDRÍA SOLO UN MENOR IMPACTO EN LA ORGANIZACIÓN DURANTE UN LARGO TIEMPO
MODERADO	4 – 6	IMPLICANDO QUE LA NO DISPONIBILIDAD TENDRÍA UN IMPACTO IMPORTANTE Y LA RECUPERACIÓN DEBE SER ALCANZADA EN DÍAS
ALTO	7 – 8	SIGNIFICANDO QUE LA NO DISPONIBILIDAD CAUSARA MAYOR PROBLEMA A LA ORGANIZACIÓN Y LA RECUPERACIÓN DEBE SER ALCANZADA EN HORAS
EXTREMO	9	SIGNIFICANDO QUE LA ORGANIZACIÓN EMPIEZA A TENER GRAVES PROBLEMAS Y LA RECUPERACIÓN DEBE SER ALCANZADA EN MINUTOS
ABSOLUTO	10	SIGNIFICANDO QUE NO SE PUEDE TOLERAR LA PERDIDA DE DISPONIBILIDAD Y LA RECUPERACIÓN DEBE SER INSTANTÁNEA

Como resultado final de la aplicación de la metodología de CRAMM se obtiene:

1. Matriz de Análisis de Riesgos.
2. Reporte de Análisis.

Matriz de análisis de riesgos

Las celdas de la matriz son empleadas para registrar evaluaciones cualitativas de impacto, vulnerabilidad y exposición al riesgo.

- **Vulnerabilidad:** Cuando los activos de información no tienen o no son suficientes las seguridades físicas y lógicas.
- **Impacto:** Es la huella que deja un atentado en los activos de información.
- **Exposición al riesgo:** Presentación de los activos de información a personas no autorizadas.

La vulnerabilidad y la exposición al riesgo de los activos de información también se basan en tablas para su interpretación y éstas son:

Tabla de exposición al riesgo

Tabla 2.4 (Tabla de exposición)

RIESGO	**VALOR**
BAJO	1 – 20
MODERADO	21 – 60
ALTO	61 – 80
EXTREMO	81 – 100

Tabla de vulnerabilidad

Tabla 2.5 (Tabla de vulnerabilidad)

NIVEL	**VALOR**
NINGUNO	0
BAJO	1 – 4
MODERADO	5 – 7
ALTO	8 – 9
EXTREMO	10

A continuación se presenta la matriz de riesgos.

Matriz de riesgos

ACTIVO DE INFORMACION			I	C	D								
1	IMPACTO 3		0	0	0								
4	2 AMENAZAS	Accidentales	I	C	D	Origen Humano	I	C	D	Intencionales	I	C	D
	VULNERABILIDAD	Terremotos	0	0	0	Errores de Utilización	0	0	0	Robo	0	0	0
		Inundaciones	0	0	0	Negligencia Personal	0	0	0	Fraude	0	0	0
		Influencias electromagnéticas	0	0	0					Espionaje	0	0	0
										Vandalismo	0	0	0
										Sabotaje externo	0	0	0
										Sabotaje interno	0	0	0
										Utilización abusiva del computador	0	0	0
										Uso no autorizado de la información	0	0	0
5	**EXPOSICION AL RIESGO**	Terremotos	0	0	0	Errores de Utilización	0	0	0	Robo	0	0	0
		Inundaciones	0	0	0	Negligencia Personal	0	0	0	Fraude	0	0	0
		Influencias electromagnéticas	0	0	0					Espionaje	0	0	0
										Vandalismo	0	0	0
										Sabotaje externo	0	0	0
										Sabotaje interno	0	0	0
										Utilización abusiva del computador	0	0	0
										Uso no autorizado de la información	0	0	0

NOTA: Los custodios de la información son responsables de categorizar sus datos en términos de su necesidad de integridad, confidencialidad y disponibilidad.

1

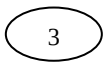
Los activos de la información son los puntos y objetivos de control, que se establecen para cada auditoría (Capitulo No. 2), que abarcan aspectos administrativos y técnicos que debe cumplir determinada área. Sin embargo, en ocasiones estos puntos de control pueden ser muy generales por lo que se sugiere dividirlos o segmentarlos de acuerdo al alcance que se desee tener.

2

La matriz evalúa tres tipos de amenazas que son:

- Amenazas originadas por errores humanos.
  - Errores de utilización.
  - Negligencia personal.
- Amenazas originadas por la naturaleza.
  - Terremotos.
  - Inundaciones.
  - Influencias electromagnéticas.
- Amenazas provocadas intencionalmente.
  - Robo.
  - Fraude.
  - Espionaje.
  - Vandalismo.
  - Sabotaje interno.
  - Sabotaje externo.
  - Utilización abusiva del computador.
  - Uso no autorizado de la información.

El impacto y la vulnerabilidad se completan de la siguiente manera:

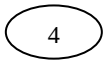


Se asigna un valor para representar el impacto potencial en el activo de información para el caso en que no se satisfaga el requerimiento de integridad, confidencialidad y disponibilidad.

Para colocar los valores del impacto se debe realizar la siguiente pregunta ¿Cual es el impacto que se produce al mantener ***(aquí se incluye el punto de control o el segmento según el alcance que se desee dar)*** para que llegue afectar la integridad, confidencialidad y disponibilidad?.

Por ejemplo: Un punto de control que se tiene en la auditoria informática para la estructura organizacional son los estándares ahora se formula la pregunta.

¿ Cual es el impacto que se produce al mantener estándares para que llegue afectar la integridad de la información ?



Para calcular la vulnerabilidad se debe tomar en consideración la probabilidad de que la amenaza, debido a las debilidades, permita que ocasione un impacto en la organización.

Al momento de asignar valores para la vulnerabilidad se debe formular la siguiente pregunta siempre recordando que el objetivo central es la información, la pregunta es.

*En caso de que ocurra **(se coloca la amenaza)**, **(aquí se incluye el punto de control o el segmento según el alcance que se desee dar)** que vulnerabilidades presenta la información en cuanto a la integridad, confidencialidad y disponibilidad.*

Por ejemplo: Un punto de control que se tiene en la auditoria informática para la estructura organizacional son los estándares ahora se formula la pregunta.

En caso de que ocurra un terremoto, los estándares que vulnerabilidades presentan a la información en cuanto a la integridad.

Es importante que cualquier medida de control, de seguridad, existente y / o introducida para reducir la probabilidad o frecuencia de la vulnerabilidad en la organización debe ser identificada y tomada en cuenta para asignar un valor.

5 El valor de la exposición al riesgo se calcula multiplicando los valores de impacto y de vulnerabilidad el resultado de dicha operación se traslada a un factor de riesgo para cada categoría de activo de información. La tabla de exposición al riesgo permite una categorización de los riesgos existentes.

Tabla de exposición al riesgo

Tabla 2.6 (Tabla de exposición al riesgo)

RIESGO	**VALOR**
BAJO	1 – 20
MODERADO	21 – 60
ALTO	61 – 80
EXTREMO	81 – 100

El reporte de análisis

El reporte de análisis consiste en dar a conocer el porcentaje que determinará si el área necesita ser auditada.

Este porcentaje se calcula de la siguiente manera: Al tener la matriz de riesgos con la información que necesaria, se procede a calcular un porcentaje lineal, es decir, se realiza una suma de un grupo de valores y se divide para el numero de valores sumados, los campos de los que se realiza la suma depende del criterio del auditor ya que se puede obtener un porcentaje de la vulnerabilidad y exposición al riesgo, además, de la integridad, confidencialidad y disponibilidad de la información. Aquí se recomienda que se obtenga un valor de toda la matriz por medio siempre de promedios lineales.

Evidentemente esta matriz es muy flexible ya que permite al auditor establecer valores adicionales de peso para una amenaza o una vulnerabilidad.

A continuación se muestra la tabla de porcentajes que ayudaran para establecer el área a ser auditada.

Tabla de auditoria

Tabla 2.7 (Tabla de auditoria)

PORCENTAJES	**VALOR**
0 – 40%	Muy deficiente
41 – 70%	Deficiente
71 – 90 %	Aceptable
91 – 100%	Correcto

Una vez determinadas las áreas a ser auditadas, se procede a realizar un examen detallado de las áreas criticas.

Examen detallado de la áreas criticas

Es la fase más importante de la Auditoria Informática, se requiere mayor tiempo que la anterior, y según sea la complejidad, se requiere de especialistas en redes, comunicaciones, herramientas para desarrollo de sistemas, etc. que sean el soporte de las actividades técnicas que haya que profundizar. El desarrollo de esta fase se la realiza exclusivamente en el campo, y es prácticamente la culminación del trabajo de auditoria.

Los procedimientos de esta fase se centran hacia la identificación de hallazgos que incluyen acciones correctivas que ameritan ser recomendadas en el informe, por tal motivo es aconsejable preparar no un programa sino tantos como áreas críticas se hayan identificado en la fase anterior, de tal suerte que se facilite su ejecución por separado por parte del auditor o especialista según sea el caso.

Para esta fase se utilizara la metodología CRMR (Evaluación de la gestión de recursos informáticos) .

Metodología CRMR (Evaluación de la gestión de recursos informáticos)

CRMR son las siglas de "Computer Resource Management Review". La traducción más adecuada sería la de "Evaluación de la gestión de recursos informáticos". En cualquier caso, esta terminología quiere destacar la posibilidad de realizar una evaluación de eficiencia de utilización de los recursos por medio del "management"[5].

El método CRMR puede aplicarse cuando se producen algunas de las situaciones que se citan:

[5] **Management** : Gerencia

- Se detecta una mala respuesta a las peticiones y necesidades de los usuarios.
- Los resultados del Centro de Procesos de Datos no están a disposición de los usuarios en el momento oportuno.
- Se genera con alguna frecuencia información errónea por fallos de datos o proceso.
- Existen sobrecargas frecuentes de capacidad de proceso.
- Existen costos excesivos de proceso en el Centro de Proceso de Datos.

Las áreas en que el método CRMR puede ser aplicado se corresponden con las sujetas a las condiciones de aplicación señaladas en el punto anterior:

- Gestión de Datos.
- Control de Operaciones.
- Control y utilización de recursos materiales y humanos.
- Interfaces y relaciones con usuarios.
- Planificación.
- Organización y administración.

Para poder cubrir el alcance que se desea dar al proceso de auditoria es necesario que se segmente al área e inclusive si el caso, así lo amerita, dividir al segmento en secciones o sub-secciones.

Los segmentos serán los puntos de control que dicta la metodología de COBIT y las secciones serán los objetivos de control de cada control (Capitulo No. 2), finalmente las sub-secciones serán utilizadas cuando se desee evaluar algo muy especifico como puede ser las partes de un manual o el contenido de un plan.

Como sugerencia se puede acotar que para llegar a trabajar con sub-secciones se debe leer y entender los puntos y controles de control.

El siguiente ejemplo ilustra de mejor manera lo anterior: En la auditoria de estructura organizacional se toma en cuenta a la Determinación de la tecnología que va a ser nuestro punto de control, los segmentos serán:

Tabla 2.8 (Tabla de segmentos)

SEGMENTOS
Definición de la arquitectura de información
Determinación de la dirección tecnológica
Definición de la organización y de las relaciones de TI

Las secciones del segmento “Determinación de la dirección tecnológica” será:

Tabla 2.9 (Tabla de secciones)

SECCIONES
Estándares de tecnología

Una vez que se establezca los segmentos, las secciones y las sub-secciones, si el caso lo amerita, se procede a armar la siguiente matriz para los segmentos. Tomando el ejemplo anterior.

Tabla 2.10 (Tabla de segmentos con promedios)

SEGMENTOS	Promedio técnico	Promedio Ponderado	Promedio Total	Resultados
Definición de la arquitectura de información	40	60	50	70
Determinación de la dirección tecnológica	40	40	40	0
Definición de la organización y de las relaciones de TI	20	0	10	0
	100	100	100	0

La primera columna indica los segmentos definidos anteriormente, la segunda columna indica el promedio técnico, este valor lo asigna el auditor informático de acuerdo a su importancia la tercera columna es el promedio ponderado que se discute entre el auditor y el auditado, en ocasiones no se llega un acuerdo entre el auditor y el auditado para este valor por lo que el auditor tiene toda la libertad de colocar el valor sin el consentimiento del auditado, la cuarta columna es el promedio total que es un promedio lineal de los dos primeros promedios la ultima columna indica resultados que proviene de la tabla 2.11.

Finalmente el resultado de toda esta tabla es un promedio ponderado en el que interactúan los valores de las columnas “promedio total” y “resultados”.

La siguiente tabla es para las secciones en la que solo se incluirá los promedios técnicos.

Tabla 2.11 (Tabla de secciones con promedios)

SECCIONES	Promedio técnico	Resultado del check list
Estándares de tecnología	40	70
	Resultado	**0**

La última columna es el resultado del check list. Este check list es el cuestionario que se realiza para evaluar a la sección cuyo valor se lo coloca en la columna con la etiqueta “Resultado del check list” el resultado de esta tabla se calcula realizando un promedio ponderado entre los valores de la columna “promedio técnico” y “Resultado del check list” .

Es importante conocer que las preguntas se establecen en función de evaluar el objetivo de control, esta evaluación incluye el verificar físicamente para otorgar el valor correspondiente.

Es conocido que en un proceso de auditoria, la experiencia del auditor juega un papel importante, además de su conocimiento técnico, la capacidad de sacar información al auditado, entre las principales características, sin embargo, la metodología que se plantea pretende dar el menor margen posible para la subjetividad esto se lo logra por medio de matrices como las siguientes:

Tabla 2.12 (Estado físico)

Valor	Descripción
1	Buen Estado
0,5	Regular Estado
0	Mal Estado

Tabla 2.13 (Tabla de seguridad de almacenamiento)

Valor	Descripción
1	Seguro
0,5	Seguridad media
0	No es seguro

Tabla 2.14 (Tabla de apoyo de Alta gerencia)

Valor	Descripción
1	Si
0,5	Parcialmente
0	No

Tabla 2.15 (Tabla de valoración de las preguntas)

Valor	Descripción
1	Muy deficiente
2	Deficiente
3	Mejorable
4	Correcto
5	Aceptable

Tabla 2.16 (Tabla de lugar de almacenamiento)

Valor	Descripción
1	Difícil acceso
0,5	Acceso medio
0	Fácil acceso

Los check list son las preguntas que permiten evaluar al segmento o la sección colocadas en una tabla como la siguiente:

Tabla 2.17 (Tabla de check list)

Check List

Ítem	Preguntas	Si	No	Observación	Referencia	Puntos

La primera columna se refiere al número de la pregunta, la segunda es donde va la pregunta, la tercera es la respuesta que se da a la pregunta por tal motivo se procura que las preguntas sean del tipo cerrada, la quinta columna es un campo donde el auditor puede colocar observaciones que servirán para evaluar a la pregunta, la siguiente columna indica código de referencia que se le asigna a un documento en particular, en caso de que exista, finalmente está la columna de puntuación de la pregunta.

Es importante recalcar que para colocar una valoración a las preguntas se debe realizar una evaluación física de la pregunta.

Las preguntas se valoran sobre 5 puntos, en caso de ser necesario, se efectuarán reglas de tres para que se tenga dicho valor, además se debe tomar en cuenta que en caso de existir valores decimales se tomara en cuenta las reglas de aproximaciones usadas en probabilidad y estadística.

Finalmente se realiza una regla de tres sencilla para sacar un porcentaje y se pasa este valor a la matriz de secciones y el resultado de esta se trasladará a la matriz de segmentos. Y de esta manera se tendrá un porcentaje de auditoria. Se debe tomar en cuenta los valores de la tabla 2.7.

Al concluir la evaluación de los segmentos y las secciones se realiza una ficha de hallazgos como la siguiente:

Tabla 2.18 (Tabla de hallazgos)

Condición	Foto de la situación real.
Criterio	Opinión sustentada del auditor
Causa	Lo que generó el problema
Efecto	Lo que produce el problema en la organización.

Comunicación de resultados

En base a los resultados obtenidos de la fase anterior (tabla No. 18), es decir, de los hallazgos descritos en las hojas de apuntes, se procede a la elaboración del borrador del informe con la correspondiente aprobación de Auditoria Interna. Finalmente se realizan las conclusiones y recomendaciones.

CAPITULO No. V

AUDITORIAS INFORMATICAS

AUDITORIA INFORMÁTICA ESTRUCTURA ORGANIZACIONAL

INTRODUCCION

Una organización es un grupo humano deliberadamente constituido en torno a tareas comunes y en función de la obtención de objetivos específicos. Para poder alcanzar los objetivos propuestos, partiendo, en la casi totalidad de los casos, de recursos limitados, entonces resulta necesaria la construcción de un **esquema o modelo,** que permita la interrelación e interacción de sus elementos.

La estructura será entonces, la herramienta que le permita a la organización alcanzar sus objetivos y de esta manera, se puede realizar el esfuerzo coordinado que lleve a la obtención de objetivos, definiendo las relaciones y aspectos más o menos estables de la organización.

En la estructura, las partes están integradas, es decir, que se relacionan de tal forma que un cambio en uno de los elementos componentes afecta y genera cambios en los demás elementos, en las relaciones entre los mismos y en la conducta de la organización toda.

OBJETIVO

- Auditar la Estructura Organizacional.

ALCANCE

Esta definido por:

- La especificación de las tareas a realizar en cada posición de trabajo.
- Determinación del sistema de autoridad.

MARCO TEORICO

Definición .- "Es el conjunto de medios que maneja la organización con el objeto de dividir el trabajo en diferentes tareas y lograr la coordinación efectiva de las mismas"[6].

Eficacia y eficiencia en la estructura organizacional

A través del diseño de la estructura de la organización se busca el logro de un adecuado grado de eficacia y eficiencia de la organización.

La estructura formal es un elemento fundamental para proporcionar un ambiente interno adecuado en la organización, en el que las actividades que desarrollan sus miembros contribuyen **al logro de los objetivos organizacionales.**

La estructura organizacional presenta dos aspectos:

- ✓ Lo *formal.* Se puede identificar con los elementos visibles, susceptibles de ser representados, modelados con el uso de diversas técnicas, que veremos más adelante, como organigramas, manuales, procedimientos, documentación de sistemas, etc.
- ✓ Lo *informal.* Se puede identificar con lo que no se ve, lo no escrito, lo que no está representado en los modelos formales; entran aquí las relaciones de poder, los intereses grupales, las alianzas interpersonales, las imágenes, el lenguaje, los símbolos, la historia, las ceremonias, los mitos y todos los atributos conectados con la cultura de la organización, que generalmente más importa para entender la vida organizacional.

[6] Mintzberg, Henry**. DISEÑO DE ORGANIZACIONES EFICIENTES**. El Ateneo, Buenos Aires (1991)

La suma de los componentes formales e informales constituye la estructura de la organización; es por eso que la estructura formal y la informal se encuentran estrechamente relacionadas. Si se define en forma adecuada, la estructura formal debe reflejar las pautas de comportamiento informal.

Se debe siempre tener en cuenta que la estructura formal deberá reflejar razonablemente el comportamiento ***real*** del sistema; es decir, debe ser representativa de la estructura informal. Si esto se altera, la estructura se convierte en una mera expresión formal de deseos.

Elementos de la estructura organizacional

1. **Especificación de las tareas a realizar:** Cada posición de trabajo y agrupamiento de las tareas similares y/o relacionadas en departamentos, los que a su vez serán agrupados en unidades mayores que los contengan, de acuerdo a su especialización, similitud o vinculación de procesos y funciones. A este proceso se lo denomina departamentalización.

2. **Fijación de los mecanismos de coordinación entre las personas:** Existen tres mecanismos de coordinación que son:

   - Adaptación mutua, o comunicación informal, que se logra a través del conocimiento de lo que cada uno debe hacer dentro de una lógica de decisiones programadas.

- Supervisión directa, que surge como consecuencia directa de la autoridad que establecerá y controlará qué, quién, cómo, cuándo y dónde debe hacerse algo; y
- Formalización o normalización, que consiste en estandarizar actividades o atributos respecto de un proceso, producto o resultado, y se plasma a través de instrumentos como los manuales, los circuitos administrativos, etc.

3. **Determinación del sistema de autoridad.** A través de éste se consolidarán:
   - los niveles jerárquicos;
   - los procesos de toma de decisiones;
   - las asignaciones de atribuciones (misiones y funciones); y
   - los alcances de las responsabilidades.

Las organizaciones poseen diferentes estructuras entre sí, y una misma organización puede ir cambiando su estructura, conforme evoluciona su número de integrantes, la especialización, el grado de concentración de la autoridad, etc. Por lo tanto, la estructura puede ser modificada toda vez que las necesidades de la organización así lo requieran; debiendo guiarse por una lógica que permita el logro de la eficacia y eficiencia organizacional.

PUNTOS DE CONTROL

Los puntos de control para esta auditoría son:

1. Definición de la arquitectura de información.
2. Determinación de la dirección tecnológica.
3. Definición de la organización y de las relaciones de T.I.
4. Comunicación de la dirección y aspiraciones de la gerencia.
5. Administración de recursos humanos.

6. Aseguramiento de cumplimiento de requerimientos externos.

Estos puntos de control permiten:

- Organizar de la mejor manera los sistemas de información.
- Aprovechar la tecnología disponible o tecnología emergente.
- Evaluar la prestación de servicios de T.I.
- Asegurar el conocimiento y comprensión del usuario sobre dichas aspiraciones.
- Maximizar las contribuciones del personal a los procesos de T.I.
- Cumplir con obligaciones legales, regulatorias y contractuales.

Además se debe tomar en cuenta ciertos lineamientos para una mejor evaluación de los puntos de control como los siguientes:

- Propiedad de la información.
- Capacidad de adecuación y evolución de la infraestructura actual.
- Monitoreo de desarrollos tecnológicos.
- Comité de dirección.
- Responsabilidades a nivel de alta gerencia o del consejo.
- Segregación de funciones.
- Roles y responsabilidades.
- Descripción de puestos.
- Niveles de asignación de personal.
- Personal clave.
- Código de ética / conducta.

- Directrices tecnológicas.
- Cumplimiento.
- Políticas de seguridad.
- Políticas de control interno.
- Reclutamiento y promoción.
- Requerimientos de calificaciones.
- Capacitación.
- Leyes, regulaciones, contratos.
- Monitoreo de evoluciones legales y regulatorios.
- Búsqueda de asistencia legal y modificaciones.

A continuación definimos los objetivos de control para cada punto de control.

Puntos y objetivos de control

1 Definición de la arquitectura de información

1.1 Niveles de seguridad

2 Determinación de la dirección tecnológica

2.1 Estándares

3 Definición de la organización y de las definiciones de TI (Tecnología de información)

3.1 Comité de planeación o dirección de la función de servicios de información.

3.2 Ubicación de los servicios de información en la organización.

3.3 Revisión de Logros Organizacionales.

3.4 Funciones y Responsabilidades.

3.5 Segregación de Funciones.

3.6 Asignación de Personal para Tecnología de Información.

3.7 Descripción de Puestos para Personal de la Función de Servicios de información.

3.8 Personal Clave de T.I.

3.9 Procedimientos para personal por contrato.

3.10 Relaciones.

4 Administración de recursos humanos

4.1 Reclutamiento y Promoción de Persona.

4.2 Personal Calificado.

4.3 Entrenamiento de Personal.

4.4 Entrenamiento Cruzado o Respaldo de personal.

4.5 Procedimientos de Acreditación de Personal.

4.6 Evaluación de Desempeño de los Empleados.

4.7 Cambios de Puesto y Despidos.

5. Aseguramiento de cumplimiento de requerimientos externos.

5.1 Revisión de Requerimientos Externos.

5.2 Prácticas y Procedimientos para el Cumplimiento de Requerimientos Externos.

5.3 Privacidad, propiedad intelectual y flujos de datos y Flujo de Datos.

5.4 Cumplimiento con los Contratos de Seguros.

6. Comunicación de la dirección y aspiraciones de la gerencia.

Responsabilidad de la Gerencia en cuanto a Políticas.

Comunicación de las Políticas de la Organización.

Recursos para la implementación de Políticas.

Mantenimiento de Políticas.

Cumplimiento de Políticas, Procedimientos y Estándares.

Estos objetivos de control se lo ubica en las divisiones que se ha realizado para esta auditoría para que de esta manera sea mas sencillo evaluar desde diferentes perspectivas a la estructura Organizacional.

La especificación de las tareas a realizar en cada posición de trabajo.

- Niveles de seguridad.
- Estándares.
- Comité de planeación o dirección de la función de servicios de información.
- Ubicación de los servicios de información en la organización.
- Revisión de Logros Organizacionales.
- Funciones y Responsabilidades.
- Segregación de Funciones.
- Descripción de Puestos para Personal de la Función de Servicios de información.
- Relaciones.

Determinación del sistema de autoridad.

- Ubicación de los servicios de información en la organización.
- Revisión de Logros Organizacionales.
- Funciones y Responsabilidades.
- Segregación de Funciones.
- Asignación de Personal para Tecnología de Información.
- Personal Clave de T.I.
- Procedimientos para personal por contrato.
- Reclutamiento y Promoción de Persona.

- Personal Calificado.
- Entrenamiento de Personal.
- Entrenamiento Cruzado o Respaldo de personal.
- Procedimientos de Acreditación de Personal.
- Evaluación de Desempeño de los Empleados.
- Cambios de Puesto y Despidos.
- Revisión de Requerimientos Externos.
- Prácticas y Procedimientos para el Cumplimiento de Requerimientos Externos.
- Privacidad, propiedad intelectual y flujos de datos.
- Cumplimiento con los Contratos de Seguros.
- Responsabilidad de la Gerencia en cuanto a Políticas.
- Comunicación de las Políticas de la Organización.
- Recursos para la implementación de Políticas.
- Mantenimiento de Políticas.
- Cumplimiento de Políticas, Procedimientos y Estándares.

PROCESO DE AUDITORIA

Se procede a seleccionar los puntos y objetivos de control que permitirán evaluar un área especifica, finalmente se debe dirigir a la capitulo No. 2 en la parte de "Examen detallado de áreas criticas".

CUESTIONARIOS DE AYUDA

CUESTIONARIO No. 1

DIRGIDAS A LA GERENCIA DE SISTEMAS DE INFORMACION.

Objetivos:

- Evaluar la definición de la arquitectura de tecnología.
- Evaluar la determinación de la dirección tecnológica.

1. Se cuenta con una definición de los niveles de seguridad para cada uno de las clasificaciones de datos.

   SI NO

2. Se implementan los niveles de seguridad para cada uno de las clasificaciones de datos.

   SI NO

3. Se realiza un mantenimiento de los niveles de seguridad para cada uno de las clasificaciones de datos.

   SI NO

4. Se realiza una definición de estándares de tecnología para la Armada.

   SI NO

5. Quien se encarga de definir estos estándares.

   .....

6. Cada que tiempo se actualizan estos estándares.

   .....

7. Quien se encarga de la difusión de estos estándares.

   .....

8. Existen estándares.

   SI NO

9. Controlan la aplicación de estos estándares.

   SI NO

CUESTIONARIO No. 2

DIRGIDAS A LA GERENCIA DE SISTEMAS DE INFORMACION.

Objetivos:

- Evaluar la definición de la organización y de las relaciones de TI.

1. Existe un comité de dirección o planeación para vigilar la función del CETEIN y sus necesidades.

   SI NO

2. Quien forma parte de este comité.

.....

3. La ubicación de la función de servicios de información en la estructura organizacional general asigna la existencia de autoridad, actitud critica e independiente.

   SI NO

4. La ubicación de la función de servicios de información en la estructura organizacional general garantiza que las soluciones de TI sean efectivas.

   SI NO

5. Establece una relación de sociedad con la alta gerencia para incrementar la capacidad de previsión, comprensión y habilidad para identificar y resolver el problema de TI.

   SI NO

6. Se revisa que la estructura organizacional cumpla continuamente con los objetivos y se adapte a las circunstancias cambiantes.

   SI NO

7. El personal de la Armada conoce sus funciones y responsabilidades en reacción a los sistemas de información.

   SI NO

8. El personal de la Armada cuenta con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas.

   SI NO

9. El personal de la Armada tiene responsabilidad con respecto a la seguridad y control interno.

   SI NO

10. Se asigna la responsabilidad de la ejecución de la función de aseguramiento de calidad a miembros del personal de la función de servicio de información.

SI NO

11. La gerencia asegura que existan sistemas de aseguramiento de calidad apropiados, controles y experiencia en comunicación dentro del grupo de aseguramiento de calidad de la función de servicios de información.

SI NO

12. La ubicación de la función de aseguramiento de calidad dentro de la función de servicios de información así como las responsabilidades y el tamaño del grupo de aseguramiento de calidad satisfacen dichos requerimientos.

SI NO

13. Se cuenta con una división de seguridad lógica y física de los activos de información.

SI NO

14. Cual es la responsabilidad de esta división.

.....

15. Se asigna responsabilidades gerenciales de seguridad adicional a niveles específicos.

SI NO

16. Se cuenta con una división / estructura para designar formalmente a los propietarios y custodios de los datos y sistemas.

SI NO

17. Las funciones y responsabilidades de esta división / estructura están claramente definidos.

SI NO

18. Los propietarios y custodios de datos y sistemas toman decisiones sobre la clasificación y derechos de acceso.

SI NO

19. Los propietarios de datos y sistemas delegan la custodia a un grupo de operación del sistema y las responsabilidades de seguridad a un administrador de seguridad.

SI NO

20. La alta gerencia implementa practicas de supervisión en la organización de servicios de información.

SI NO

21. Las practicas de supervisión permiten asegurar que las funciones y responsabilidades son llevadas a cabo apropiadamente.

SI NO

22. Cuantas personas resuelven un proceso critico.

.....

23. El personal que trabaja en la Armada realiza otras tareas a parte de las tareas asignadas a su puesto de trabajo.

SI NO

24. Se mantiene una segregación de funciones entre las siguientes funciones:
    - Uso de sistemas de información.
    - Entrada de datos.
    - Operación de cómputo.
    - Administración de redes.
    - Administración de sistemas.
    - Desarrollo y mantenimiento de sistemas.
    - Administración de cambios.
    - Administración de seguridad; y
    - Auditoría de seguridad.

25. Los requerimientos de personal para la función de tecnologías de información son revisadas periódicamente.

SI NO

26. Se evalúan dichos requerimientos

SI NO

27. El proceso de asignación de personal es adecuando y se apega a las reales necesidades de la función.

SI NO

28. Se actualiza las descripciones de los puestos para el personal de la función de sistemas de información regularmente.

SI NO

29. La descripción de puestos para la función de servicios de información delinean claramente la responsabilidad y autoridad.

SI NO

30. La descripción de puestos para la función de servicios de información incluyen definiciones de las habilidades y la experiencia necesaria para el puesto.

SI NO

31. La descripción de puestos para la función de servicios de información incluyen la definición e identifican al personal clave de TI.

SI NO

32. Se cuenta con procedimientos relevantes para controlar las actividades de consultores y de personal externo contratado para la función de sistemas de información.

SI NO

CUESTIONARIO No. 3

PREGUNTAS DIRIGIDAS A LA GERENCIA DE SISTEMAS DE INFORMACION.

Objetivos:

- Evaluar la comunicación de la dirección y aspiraciones de la gerencia.

1. La gerencia de sistemas de información plantea políticas que cubran metas y directrices generales.

SI NO

2. La gerencia de sistemas de información desarrolla políticas que cubran metas y directrices generales.

SI NO

3. La gerencia de sistemas de información documenta políticas que cubran metas y directrices generales.

SI NO

4. La gerencia de sistemas de información promulga políticas que cubran metas y directrices generales.

SI NO

5. La gerencia de sistemas de información controla políticas que cubran metas y directrices generales.

SI NO

6. Las políticas organizacionales son comunicadas

SI NO

7. Las políticas organizacionales son comprendidos por los niveles de la organización.

SI NO

8. Se evalúa que la organización haya comprendido las políticas.

SI NO

9. Se destina recursos para la implementación de las políticas.

SI NO

10. Se toma en cuenta el tiempo que se toma en implementar las políticas.

SI NO

11. Se cuenta con un proceso para revisiones periódicas de las políticas, estándares, directrices y procedimientos.

SI NO

12. Estas revisiones periódicas se realizan cada que tiempo.

.....

13. Se establece procedimientos apropiados para determinar si el personal comprende los procedimientos y políticas implementados.

SI NO

14. El personal cumple con los procedimientos y políticas de la Armada.

SI NO

15. Se documenta una filosofía de calidad así como políticas y objetivos que sean consistentes con la filosofía y las políticas de la corporación a este respeto.

SI NO

16. Se mantiene la filosofía de calidad así como políticas y objetivos que sean consistentes con la filosofía y las políticas de la corporación a este respeto.

SI NO

17. La filosofía de calidad, las políticas y los objetivos son comprendidos implementados y mantenidos a todos los niveles de la función de servicios de información.

SI NO

18. Quien desarrolla las políticas de seguridad y control interno.

.....

19. Las políticas cumplen con los objetivos generales del negocio.

SI NO

20. Las políticas están dirigidas a minimizar el riesgo a través de medidas preventivas.

SI NO

21. Las políticas están dirigidas a identificación oportuna de irregularidades.

SI NO

22. Las políticas están dirigidas a limitar las pérdidas.

SI NO

23. Las políticas están dirigidas a una recuperación oportuna.

SI NO

24. Las medidas se basan en un análisis costo beneficio.

SI NO

25. Las políticas de seguridad y control interno especifican el propósito y objetivos.

SI NO

26. Las políticas de seguridad y control interno especifica la estructura gerencial.

SI NO

27. Las políticas de seguridad y control interno especifica el alcance dentro de la organización.

SI NO

28. Las políticas de seguridad y control interno especifica la definición y asignación de responsabilidades para su implementación en todos los niveles.

SI NO

29. Las políticas de seguridad y control interno especifica la definición de multas y de acciones disciplinarias asociadas con la falta de cumplimiento.

SI NO

30. Se cuenta con una política de propiedad intelectual.

SI NO

31. Las políticas cubren aspectos como desarrollo de software interno y desarrollo de software contratado a externos.

SI NO

32. Se cuentan con políticas para situaciones especificas.

SI NO

33. Se documentan estas políticas con respecto a tratamientos de actividades, aplicaciones, sistemas de tecnología particular.

SI NO

CUESTIONARIO No. 4

PREGUNTAS DIRIGIDAS A LA GERENCIA DE SISTEMAS DE INFORMACION.

Objetivos:

- Evaluar la administración de los recursos humanos.

1. Se cuentan con procesos de reclutamiento y promoción de personal

   SI NO

2. Estos procesos tienen criterios, objetivos y se considera factores como:
   - Educación
   - Experiencia
   - Responsabilidad.
3. Dichos procesos se alinean con las políticas y procedimientos generales de la Armada a este respecto.

   SI NO

4. Se verifica que el personal que lleva a cabo tareas específicas esté calificado tomando como base una educación, entrenamiento y / o experiencia apropiados, según se requiera.

   SI NO

5. La gerencia alienta al personal para que participen, como miembro, en organizaciones profesionales.

   SI NO

6. Se proporciona entrenamiento y capacitación constantes al personal.

   SI NO

7. Los programas de educación y entrenamiento se revisan regularmente.

   SI NO

8. Se cuenta con personal de respaldo en caso de ausencias.

   SI NO

9. Se realiza un entrenamiento cruzado adecuado para suplir las ausencias de personal.

   SI NO

10. Se tiene procedimientos de revisión ó acreditación de seguridad antes de ser contratado, transferido o promovido.

    SI NO

11. Se toma en cuenta el grado de sensibilidad del puesto para aplicar un procedimiento mas riguroso de acreditación de seguridad.

    SI NO

12. Se cuenta con un proceso de evaluación del empleado.

    SI NO

13. Dicho proceso de evaluación se lleva a cabo regularmente según los estándares establecidos y las responsabilidades especificas del puesto.

    SI NO

14. Los empleados reciben asesoría sobre su desempeño o su conducta.

    SI NO

15. Se cuenta con acciones con respecto a cambios de puestos y despidos.

    SI NO

AUDITORIA INFORMÁTICA P.E.T.I

INTRODUCCION

El riesgo de incorporar tecnología de información (TI) se ha incrementado en la Armada. Esto se debe principalmente a que la planeación y la planeación estratégica, prácticamente no existen. Las tendencias actuales de desarrollo de TI en el mercado, se han caracterizado por esforzarse en automatizar el "desorden". Muy poco esfuerzo es puesto en especificar la estrategia de negocios y en construir un modelo de la organización, como precursores en la determinación de requerimientos de TI.

Las enormes sumas que las empresas dedican a las tecnologías de la información en un crecimiento del que no se vislumbra el final y la absoluta dependencia de las mismas al uso correcto de dicha tecnología hace necesario que se realice una evaluación al plan estratégico de TI (P.E.T.I), ya que en el se encuentran los objetivos y metas de la Armada, en un período de tiempo, además los recursos humanos, materiales y económicos que serán necesarios para alcanzar estos objetivos y metas.

OBJETIVOS

- Auditar la definición del P.E.T.I
- Auditar la definición de la arquitectura de información.
- Auditar la determinación de la dirección tecnológica.

ALCANCE

Esta dado por la definición del P.E.T.I, arquitectura de información y la determinación de la dirección tecnológica.

MARCO TEORICO

El desarrollo de T.I es visto por los expertos del área, de Tecnología de información, como un conjunto de procesos de diseño individuales. Las aplicaciones son construidas para satisfacer metas a corto plazo o problemas inmediatos. No se establece claramente una estrategia de TI, un plan o curso, y tampoco se considera la visión global de los recursos con que cuenta la organización.

El P.E.T.I consiste en un proceso de planeación dinámico, en el que las estrategias sufren una continua adaptación, innovación y cambio, que se refleja en los elementos funcionales que componen toda la organización.

El P.E.T.I (Plan Estratégico de Tecnologías de Información) es ampliamente reconocido como una herramienta para ordenar los esfuerzos de incorporación de TI, ya que establece las políticas requeridas para:

- Controlar la adquisición, el uso y la administración de los recursos de TI.
- Integra la perspectiva de negocios/organizacional con el enfoque de TI.
- Establece un desarrollo informático que responde a las necesidades de la organización y contribuye al éxito de la Armada.

El desarrollo de este plan está relacionado con la creación de un plan de transformación, que va del estado actual en que se encuentra la organización, a su estado final esperado de automatización, esto, en concordancia con la estrategia de negocios y con el propósito de crear una ventaja competitiva.

El P.E.T.I se la ha dividido en 3 partes principales que son:

1. Definición del plan estratégico.
2. Arquitectura de información.
3. Dirección tecnológica.

PUNTOS DE CONTROL

Los puntos de control para esta auditoría son:

1. Definición de un plan estratégico de tecnología de información.
2. Definición de la arquitectura de información.
3. Determinación de la dirección tecnológica.

Estos puntos de control permiten:

- Satisfacer los requerimientos de la Armada para lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, así como para asegurar sus logros futuros.
- Organizar de la mejor manera los sistemas de información.
- Aprovechar la tecnología disponible o tecnología emergente.

Además se debe tomar en cuenta ciertos lineamientos para una mejor evaluación de los puntos de control:

- Definición de objetivos de negocio y necesidades de T.I.
- Inventario de soluciones tecnológicas e infraestructura actual.
- Servicios de vigilancia tecnológica.
- Cambios organizacionales.
- Estudios de factibilidad oportunos.
- Documentación.
- Diccionario de datos.
- Reglas de sintaxis de datos.
- Propiedad de la información.
- Capacidad de adecuación y evolución de la infraestructura actual.
- Monitoreo de desarrollos tecnológicos.
- Contingencias.
- Planes de adquisición.

A continuación definimos los objetivos de control para cada punto de control.

Puntos y objetivos de control

1 Definición de un plan estratégico de tecnología de información

Tecnología de Información como parte del Plan de la Organización a corto y largo plazo.

Plan a largo plazo de Tecnología de Información - Enfoque y Estructura.

Cambios al Plan a largo plazo de Tecnología de Información.

Planeación a corto plazo para la Función de Servicios de Información.

Evaluación de Sistemas Existentes.

2 Definición de la arquitectura de información

2.1 Modelo de la Arquitectura de Información

2.2 Diccionario de Datos y Reglas de Sintaxis de Datos de la Corporación

2.3 Esquema de Clasificación de Datos

Niveles de Seguridad

3 Determinación de la dirección tecnológica

3.1 Planeación de la Infraestructura Tecnológica

3.2 Contingencias en la Infraestructura Tecnológica

3.3 Planes de Adquisición de Hardware y Software

3.4 Estándares de Tecnología

Estos objetivos de control se lo ubica en las divisiones que se ha realizado para esta auditoría para que de esta manera sea mas sencillo evaluar desde diferentes perspectivas a las redes y comunicaciones.

Definición del plan estratégico.

- Tecnología de Información como parte del Plan de la Organización a corto y largo plazo.
- Plan a largo plazo de Tecnología de Información - Enfoque y Estructura.
- Cambios al Plan a largo plazo de Tecnología de Información.
- Planeación a corto plazo para la Función de Servicios de Información.
- Evaluación de Sistemas Existentes.

Arquitectura de información.

- Modelo de la Arquitectura de Información.
- Diccionario de Datos y Reglas de Sintaxis de Datos de la Corporación.
- Esquema de Clasificación de Datos.
- Niveles de Seguridad.

Dirección tecnológica.

- Planeación de la Infraestructura Tecnológica .
- Contingencias en la Infraestructura Tecnológica.
- Planes de Adquisición de Hardware y Software.
- Estándares de Tecnología.

PROCESO DE AUDITORIA

Se procede a seleccionar los puntos y objetivos de control que permitirán evaluar un área especifica, finalmente se debe dirigir a la capitulo No. 2 en la parte de "Examen detallado de áreas criticas".

CUESTIONARIOS DE AYUDA

CUESTIONARIO No. 1

PREGUNTAS DIRIGIDAS AL JEFE DE LA GERENCIA DE FUNCIONES DE SERVICIOS DE INFORMACIÓN

Objetivos:

- Evaluar la definición de un plan estratégico de tecnología de información.
- Evaluar la definición de una arquitectura de información.
- Evaluar la determinación de la dirección de tecnología .

1. Los planes a largo y corto plazo satisfacen la misión y las metas de la Armada.

   SI NO

2. Los problemas de TI así como las oportunidades son evaluadas adecuadamente y reflejadas en los planes de largo y corto plazo de la Armada.

   SI NO

3. La gerencia de la función de información implementa un proceso de planeación a largo plazo.

   SI NO

4. La gerencia de la función de información establece y aplica un enfoque estructurado al proceso de planeación a largo plazo.

   SI NO

5. En el proceso de planeación cual de los siguientes aspectos son cubiertos y tomados en cuenta:
   a. Modelo de organización y sus cambios.
   b. Distribución geográfica
   c. Evaluación tecnológica.

d. Costos.

e. Requerimientos legales y regulatorios.

f. Requerimientos de terceras partes del mercado.

g. El horizonte de planeación.

h. Reingeniería del proceso del negocio.

i. Asignación del personal.

6. Los planes a largo y corto plazo hacen referencia a otros planes como por ejemplo Planes de calidad de la organización, plan de manejo de riesgos de información, etc.

SI NO

7. La gerencia de la función de información establece un proceso para modificar oportunamente y con precisión el plan a largo plazo de TI con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la TI.

SI NO

8. Los planes a corto plazo forman parte de algún plan a largo plazo.

SI NO

9. Los planes a corto plazo son modificados de acuerdo a una metodología y se ajustan a las necesidades de la Armada.

SI NO

10. La gerencia de la función de información evalúa los sistemas existentes en términos de nivel de automatización de negocio, funcionalidad, Estabilidad, complejidad, costo, fortaleza y debilidad. Para de esta manera determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.

SI NO

11. La gerencia de la función de información crea y actualiza regularmente un modelo de arquitectura de información.

SI NO

12. El modelo de arquitectura de información abarca el modelo de datos corporativos y los sistemas de información asociados.

SI NO

13. El modelo de arquitectura de información conserva consistencia con el plan a largo plazo.

SI NO

14. La gerencia de la función de información crea y establece un diccionario de datos que incorpore reglas de sintaxis de datos de la organización.

SI NO

15. Se cuenta con un marco referencial de clasificación general relativo a la ubicación de daos en clases de información así como a la asignación de propiedad.

SI NO

16. Las reglas de acceso para las clases están definidas apropiadamente.

SI NO

17. Se ha definido, implementado y mantenido niveles de seguridad para cada uno de las clasificaciones de datos.

SI NO

18. La gerencia de la función de información crea y actualiza regularmente un plan de infraestructura tecnológica que concuerde con los planes a largo y corto plazo de TI.

SI NO

19. El plan de infraestructura tecnológica abarca aspectos tales como:
    a. Arquitectura de sistemas.
    b. Dirección tecnológica.
    c. Estrategias de migración.

20. Durante el desarrollo y mantenimiento del plan de infraestructura tecnológica se toma en cuenta factores como monitoreo de tendencias futuras y condiciones regulatorias.

SI NO

21. Se evalúa la contingencia del plan de Infraestructura Tecnológica.

SI NO

22. Los planes de adquisición de hardware y software están establecidos.

SI NO

23. Se toma en cuenta el plan de infraestructura tecnología para definir normas de tecnología para fomentar la estandarización.

SI NO

AUDITORIA INFORMÁTICA SEGURIDADES

INTRODUCCION

Cada día es mayor la importancia de la información, especialmente relacionada con sistemas basados en el uso de tecnologías de la información y comunicaciones, por lo que el impacto de los fallos, los accesos no autorizados, la revelación de la información y otras incidencias, tienen un impacto mucho mayor que hace unos años; de ahí la necesidad de protecciones adecuadas para todo aquello que involucra la correcta protección de la información.

OBJETIVOS

- Auditar las seguridades físicas de las T.I.
- Auditar las seguridades lógicas de las T.I.

ALCANCE

El alcance esta dado en las seguridades físicas y lógicas.

MARCO TEORICO

Seguridad física

El objetivo es el de proteger los sistemas tanto en la parte de hardware, software, documentación y medios magnéticos de los riesgos por pérdidas, extravíos o por daños físicos. Así mismo de los potenciales riesgos se pueden dar en el acceso de personal no autorizado sin los controles adecuados de seguridad física; en los incendios; en las interrupciones de energía eléctrica; en inundaciones por filtraciones de agua y, en los controles de acceso lógico.

Los aspectos que involucran la Seguridad Física son:

- Control de Acceso
- Seguridad contra Incendios
- Suministro de Energía
- Aire Acondicionado
- Detección de Agua
- Guardias de Seguridad
- Telecomunicaciones

Aunque la inversión en sistemas de control de acceso no debe ser necesariamente onerosa como la implantación de vidrios a pruebas de balas, guardias armados las 24 horas del día o cámaras de video; la Armada si debería contemplar controles adecuadamente razonables para evitar el acceso de individuos e incluso de personal "no autorizado" al centro de procesamiento o a las áreas de manejo de datos o información oficial y exclusiva.

Los accesos deben ser otorgados sobre la base de la necesidad mínima y dependiendo de los casos bajo la supervisión del Responsable de Sistemas. Cuando se reasigne personal a otras funciones en las que no requieran del acceso que tenían previamente autorizado; el permiso debe ser revocado una vez que la persona sea reasignada en sus funciones. Así mismo en el periodo de vacaciones del personal debe aplicarse este mismo concepto.

Las movilizaciones de equipos o medios magnéticos deben ser realizadas sólo por personal autorizado y deben seguir el procedimiento de control de movilizaciones de equipos.

El guardia de seguridad debe asegurarse que las movilizaciones de equipos o medios magnéticos tanto de ingreso como de egreso se efectúen con las autorizaciones del caso.

El personal que corresponda a la categoría de visitantes y que requieran movilizarse por el centro de procesamiento o afines deberán utilizar una tarjeta que indique su calidad de "visitantes" y estar siempre escoltados o supervisados por personal de la institución y su ingreso y salida debe quedar registrado en una bitácora del área.

La limpieza y aseo del centro de procesamiento y afines debe efectuarse en presencia del personal de la institución. Dicho personal de limpieza debe ingresar previo a la identificación ante el guardia de seguridad quien debe constatar su nombre dentro del registro del personal externo a la empresa y el horario autorizado para su acceso.

PUNTOS DE CONTROL

Los puntos de control para esta auditoría son:

1. Definición de la organización y de las relaciones de T.I.
2. Administración de los recursos humanos.
3. Adquisición y mantenimiento de arquitectura de tecnología.
4. Administración de cambios.
5. Administración de servicios prestados por terceros.
6. Garantizar la seguridad de sistemas.
7. Administración de instalaciones.

Estos puntos de control permiten:

1. Evaluar la prestación de servicios de T.I.
2. Maximizar las contribuciones del personal a los procesos de T.I.
3. Evaluar acuerdos de servicio con terceras partes.
4. Asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos.
5. Salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida.
6. Evaluar el ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales o fallas humanas.
7. Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios.
8. Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores.

Además se debe tomar en cuenta ciertos lineamientos para una mejor evaluación de los puntos de control:

- Roles y responsabilidades.
- Procedimientos de acreditación.
- Acuerdos de servicio con terceras partes.
- Acuerdos de confidencialidad.
- Autorización.
- Autenticación.
- Acceso.
- Perfiles e identificación de usuarios.

- Administración de llaves criptográficas.
- Acceso a instalaciones.
- Identificación del centro de cómputo.
- Seguridad física.
- Protección contra amenazas ambientales.
- Mantenimiento preventivo de hardware.
- Seguridad del software de sistema, instalación.
- Procedimientos de categorización, priorización y emergencia.

A continuación definimos los objetivos de control para cada punto de control.

Puntos y objetivos de control

1. Definición de la organización y de las definiciones de TI (Tecnología de información)

    1.1 Responsabilidad de la Seguridad Lógica y Física

2. Administración de recursos humanos

    a. Procedimientos de Acreditación de Personal.

3. Adquisición y mantenimiento de arquitectura de tecnología

    a. Mantenimiento preventivo para hardware

    b. Seguridad del software del sistema.

    3.2 Instalación del Software del Sistema

4. Administración de cambios

    a. Mantenimiento autorizado

5. Administración de servicios prestados por terceros

    5.1 Relaciones de seguridad

6. Garantizar la seguridad de sistemas

    a. Identificación, Autenticación y Acceso

    b. Administrar medidas de seguridad.

    c. Seguridad de Acceso a Datos en Línea.

    d. Sendero Seguro.

7. Administración de instalaciones

    7.1 Seguridad Física.

    7.2 Discreción de las Instalaciones de Tecnología de Información.

    7.3 Escolta de Visitantes.

    7.3 Protección contra factores ambientales.

    7.4 Suministro Ininterrumpido de energía.

Estos objetivos de control se lo ubica en las divisiones que se ha realizado para esta auditoría para que de esta manera sea mas sencillo evaluar desde diferentes perspectivas a las redes y comunicaciones.

Seguridades Físicas

- Responsabilidad de la Seguridad Lógica y Física.
- Procedimientos de Acreditación de Personal.

- Relaciones de seguridad.
- Administrar medidas de seguridad.
- Identificación, Autenticación y Acceso.
- Discreción de las Instalaciones de Tecnología de Información.
- Seguridad Física.
- Escolta de Visitantes.
- Protección contra factores ambientales.
- Suministro Ininterrumpido de energía.

Seguridades lógicas

- Responsabilidad de la Seguridad Lógica y Física.
- Procedimientos de Acreditación de Personal.
- Relaciones de seguridad.
- Administrar medidas de seguridad.
- Identificación, Autenticación y Acceso.
- Seguridad de Acceso a Datos en Línea.
- Sendero Seguro.

PROCESO DE AUDITORIA

Se procede a seleccionar los puntos y objetivos de control que permitirán evaluar un área especifica, finalmente se debe dirigir a la capitulo No. 2 en la parte de "Examen detallado de áreas criticas".

CUESTIONARIOS DE AYUDA

CUESTIONARIO No. 1

PREGUNTAS DIRIGIDAS LA FUNCION DE SERVICIOS DE INFORMACION.

Objetivos:

- Verificar que se cuente con definición de responsabilidades de la seguridad física y lógica.
- Evaluar el cumplimiento de las políticas, procedimientos y directrices en seguridad lógica y física.

1. Existe un documento en el que se detalle las responsabilidades de la seguridad lógica y física .

   SI NO

2. Se controla que las políticas, procedimientos y directrices en seguridad lógica y física se cumplan.

   SI NO

3. Se cumple con el procedimiento de acreditación personal

   SI NO

CUESTIONARIO No. 2

PREGUNTAS DIRIGIDAS LA FUNCION DE SERVICIOS DE INFORMACION.

Objetivos:

- Evaluar las relaciones de seguridad que se tiene como proveedores de servicio.
- Evaluar la seguridad de sistemas

1. Se cumple con acuerdos de seguridad

   SI NO

2. Las medidas de seguridad se encuentren en línea con los requerimientos de negocio.

   SI NO

3. Se tienen políticas de cambios de passwords:

   SI NO

4. Los puertos de las computadoras están debidamente cerrados.

   SI NO

5. En las computadoras están restringidos las conexiones telefónicas (dial-up).

   SI NO

6. Se cuenta con mecanismos adecuados para autentificación de usuarios.

   SI NO

7. Se cuenta con procedimientos para conservar la efectividad de los mecanismos de autenticación y acceso.

   SI NO

8. Se cuenta con canales canales o senderos seguros *(trusted path*s).

   SI NO

9. En dichos canales se cuentan con encriptamiento entre usuarios - usuarios.

   SI NO

10. En dichos canales se cuentan con encriptamiento entre sistemas - sistemas.

    SI NO

CUESTIONARIO No. 3

PREGUNTAS DIRIGIDAS LA FUNCION DE SERVICIOS DE INFORMACION.

Objetivos:

- Evaluar la seguridad en las instalaciones.

1. Se cuenta con tarjetas magnéticas para el ingreso de personal a zonas restringidas

   SI NO

2. Se cuenta con sensores de movimiento en las zonas restringidas.

   SI NO

3. La ubicación física de las instalaciones es de conocimiento publico

   SI NO

4. La ubicación física de las instalaciones es la apropiada.

SI NO

5. La ubicación de los respaldos esta ubicado en el mismo edificio

SI NO

6. Se cuenta con escoltas para los visitantes.

SI NO

7. Estos escoltas están todo el tiempo de visita

SI NO

8. Se cuenta con detectores de humo

SI NO

9. Se cuenta con extintores.

SI NO

10. Los extintores son recargados periódicamente.

SI NO

11. El piso de los centros de computo es alfombrado.

SI NO

12. Se cuenta generador de luz eléctrica.

SI NO

13. Se cuenta con detectores de humo

SI NO

14. Se cuenta con extintores.

SI NO

15. Los extintores son recargados periódicamente.

SI NO

16. El piso de los centros de computo es alfombrado.

SI NO

17. Poseen bitácoras de operación.

SI NO

CUESTIONARIO No. 4

PREGUNTAS DIRIGIDAS LA FUNCION DE SERVICIOS DE INFORMACION.

Objetivos:

- Realizar una evaluación al proceso de mantenimiento de hardware y software.
- Evaluación al proceso de instalación del software.

1. Se realiza mantenimiento preventivo de hardware.

   SI NO

2. Se registra dicho mantenimiento.

   SI NO

3. Se utiliza herramientas de hardware y software adecuadas para realizar dicho mantenimiento.

   SI NO

4. Existen procedimientos para asegurar que el software del sistema es instalado de acuerdo al marco de referencia de adquisición y mantenimiento de la infraestructura tecnológica

   SI NO

5. Las pruebas son hechas antes de autorizarse su utilización en ambiente de producción

   SI NO

6. El personal de mantenimiento tiene asignaciones específicas y su trabajo es monitoreado apropiadamente

   SI NO

CUESTIONARIO No. 5

PREGUNTAS DIRIGIDAS LA FUNCION DE SERVICIOS DE INFORMACION.

Objetivos:

- Evaluar el proceso de control interno.

1. Existe un monitoreo de la efectividad de los controles internos

SI NO

2. Poseen acciones correctivas

SI NO

3. Los controles internos operan rápidamente para re-saltar errores e inconsistencias

SI NO

4. Los controles internos son corregidos antes de que impacten a la producción

SI NO

AUDITORIA DE REDES Y COMUNICACIONES

INTRODUCCION

Dentro de la organización una de las partes mas sensibles es el área de redes y comunicaciones ya que este es el medio mas usado por los "amigos de lo ajeno" para producir daños de cualquier índole.

La seguridad de las redes y comunicaciones no depende exclusivamente del fiel cumplimiento de políticas y estándares, ni del grado de capacitación que tenga el personal para administrarlas sino de la constante revisión de las seguridades que se tengan para esta área.

OBJETIVOS

1. Auditar la determinación de la dirección tecnológica.
2. Auditar la continuidad del servicio.
3. Auditar el apoyo y asistencia a los clientes de tecnología de información.
4. Auditar la configuración de redes y comunicaciones.
5. Auditar la seguridad de los sistemas y de la información.

ALCANCE

Esta metodología pretende dar lineamientos de índole general para partir hacia lo especifico, para un proceso de auditoria informática, por dicha razón se tomará en cuenta tres áreas que son:

- Gerencia

- Red Física.
- Red Lógica.

Gerencia

La función de gerencia de redes y comunicaciones tiene un grave problema que consiste en que el directivo informático tiene amplios conocimientos de proceso de datos pero no siempre sus habilidades en temas de comunicaciones están a la misma altura, en contra parte, los informáticos a cargo de las comunicaciones suelen auto considerarse exclusivamente técnicos por lo que, el riesgo de una deficiente gerencia de comunicaciones en el esquema organizativo existe.

La función de gestión de redes y comunicaciones debe estar claramente definida, debiendo ser responsable en general de las siguientes áreas.

- Gestión de red.
- Inventario de equipamiento.
- Normativa de conectividad.
- Monitorización de las comunicaciones, registro y resolución de problemas.
- Servicios de transporte, balanceo de tráfico entre rutas y selección de equipamiento.
- Participación activa en la estrategia de proceso de datos, fijación de estándares y evaluación de necesidades en comunicaciones.

Red Física

Son aquellas instalaciones físicas por donde circulan los datos.

Red Lógica

Cuando un equipo se comunica con otro lo hace mediante la red de comunicaciones, a ésta red se denomina Red Lógica, que es necesario monitorizar la red, revisar los errores o situaciones anómalas que se producen y tener establecidos los procedimientos para detectar y aislar equipos en situación anómala.

MARCO TEORICO

Para auditar esta área es importante que se tenga conocimiento general de comunicaciones y redes para lo cual debemos referirnos al modelo adoptado por la ISO (Organización internacional de estándares) que es el Modelo OSI (Open Systems Interconection).

Modelo OSI

El Modelo OSI abarca una serie de eventos importantes que se producen durante la comunicación entre sistemas. Además proporciona las normas básicas empíricas para una serie de procesos distintos de conexión de red como:

- El modelo en que los datos se traducen a un formato apropiado para la arquitectura de red que se esta utilizando.
- El modo en que la PC u otro dispositivo de red se comunican.
- El modo en que los datos se transmiten entre diferentes dispositivos y la forma en que se resuelve la secuenciación y comprobación de errores.

- El modo en que el direccionamiento lógico de los paquetes pasa a convertirse en el direccionamiento físico que proporciona la red.

El modelo OSI ofrece mecanismos y reglas que permiten resolver todas las cuestiones anteriores. Las capas de este modelo describen el proceso de transmisión de los datos dentro de una red. Este modelo consta de 7 capas que son:

1. **Físico:** Transforma la información en señales físicas adaptadas al medio de comunicación.
2. **Enlace:** Transforma los paquetes de información en tramas adaptadas a los dispositivos físicos sobre los cuales se realiza la transmisión.
3. **Red:** Establece las rutas por las cuales se puede comunicar el emisor con el receptor, lo que se realiza mediante el envío de paquetes de información.
4. **Transporte:** Comprueba la integridad de los datos transmitidos.
5. **Sesión:** Establece los procedimientos de aperturas y cierres de sesión de comunicaciones, así como información de la sesión en curso.
6. **Presentación:** Define el formato de los datos que se van a presentar a la aplicación.
7. **Aplicación:** Es donde la aplicación que necesita comunicaciones enlaza, mediante API (Application Program Interface) con el sistema de comunicaciones.

Estas 7 capas nos ayudarán a dividir a este capitulo.

El modelo OSI permite que cada capa trabaje sin tener que preocuparse de que es lo que hagan las capas superiores y las inferiores; Cada capa se comunica con su igual en el

interlocutor, con un protocolo de comunicaciones específico. Entre cada par de capa N y capa N-1 esta perfectamente definido el paso de la información que se produce dentro de la misma maquina, con métodos clásicos de programación local.

Para establecer una comunicación, la información atraviesa descendentemente la pila formada por las 7 capas, atraviesa el medio físico y asciende a través de las 7 capas en la pila de destino. Por tanto, cada capa tiene unos métodos prefijados para comunicarse con las inmediatamente inferior y superior. De esta manera, se aíslan los protocolos que se utilizan en unas capas con los protocolos que se utilizan en otras.

Habitualmente hasta en las 3 primeras capas (Físico, Red, Enlace), se definen las redes LAN (Local Area Network), MAN (Metropolitan Area Network) y WAN (Wide Area Network).

Las funcionalidades de estos tres tipos de redes son similares variando fundamentalmente en un parámetro que es la Distancia entre el emisor y el receptor. Así se tiene que las redes LAN se enmarcan dentro del edificio, las MAN dentro de un campus o zona urbana y las WAN no tienen distancia.

Riegos y vulnerabilidad

Los sistemas en comunicación en general tiene el problema de que la información transita por lugares que físicamente están alejados de las personas responsables. Por dicha razón el compromiso de seguridad tiene que ser muy alto ya que no existen procedimientos físicos para garantizar la inviolabilidad de la información.

En general en redes de comunicación existe 3 tipos de incidencias:

1. Alteración de bits: Por error en los medios de transmisión, una trama puede sufrir variación en parte de su contenido.
2. Ausencia de tramas: Por error en el medio, o algún nodo o por sobrecarga, alguna trama puede desaparecer en el camino del emisor al receptor.
3. Alteración de secuencia: El orden en el que se envían y se reciben las tramas no coincide.

Es importante identificar que los mayores riesgos, para interceptar la información, son:

1. Indagación: Un mensaje puede ser leído por un tercero, obteniendo la información que contenga.
2. Suplantación: Un tercero puede introducir un mensaje espurio que el receptor cree proveniente del emisor legítimo.
3. Modificación: Un tercero puede alterar el contenido de un mensaje.

Por este tipo de actuaciones dolosas, en el caso de redes WAN y MAN la única medida prácticamente efectiva es la criptografía y para redes LAN se usa mucho las medidas de control de acceso a medios físicos de la red e instalaciones.

Es importante conocer que actualmente en los edificios para que exista intercambio de información entre usuarios existen sistemas de cableado integral. Éstos se dividen según su

ámbito. En cada zona se tienden cables desde un armario distribuidor a cada uno de los puestos. A este cableado se le denomina “Cableado de planta”. Los armarios se comunican entre si y con las salas de computadoras a este cableado se lo denomina “Cableado de troncal” y el “Cableado de ruta” es aquel que va desde las salas de computación hacia los transportistas de datos (Telefónicas o PTTs), saliendo los cables al exterior del edificio.

PUNTOS DE CONTROL

Los puntos de control para esta auditoria son:

1. Determinación de la dirección tecnológica.
2. Garantizar la seguridad de los sistemas.
3. Apoyo y asistencia a los clientes de tecnología de información.
4. Administración de la configuración.
5. Administración de problemas e incidentes.
6. Administración de datos.

Estos puntos de control permiten:

- Aprovechar la tecnología disponible o tecnología emergente.
- Salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida.
- Asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente.

- 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.
- Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir cualquier recurrencia.
- Asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento

Además se debe tomar en cuenta ciertos lineamientos para una mejor evaluación de los puntos de control:

- Capacidad de adecuación y evolución de la infraestructura actual.
- Consultas de usuarios y respuesta a problemas.
- Administración de cambios en la configuración.
- Chequeo de software no autorizado.
- Autorizaciones de acceso.
- Autenticación e integridad de la información.
- Perfiles e identificación de usuarios.
- Administración de llaves criptográficas.
- Manejo, reporte y seguimiento de incidentes.
- Firewalls.
- Reportes de incidentes.
- Pistas de auditoría de problemas y soluciones.
- Controles de documentos fuente.

- Controles de entrada.
- Controles de procesamiento.
- Controles de salida.

A continuación definimos los objetivos de control para cada punto de control.

Puntos y objetivos de control

1. Determinación de la tecnología

Estándares de tecnología

2. Apoyo y asistencia para los clientes de tecnología de información

2.1 Buró de Ayuda

2.2 Registro de Preguntas del Usuario

3 Garantizar la seguridad de sistemas

3.1 Identificación, Autenticación y Acceso

3.2 Seguridad de Acceso a Datos en Línea

3.3 Revisión Gerencial de Cuentas de Usuario

3.4 Vigilancia de Seguridad

3.5 Clasificación de Datos

3.6 Reportes de Violación y de Actividades de Seguridad

3.7 Re acreditación

3.8 Confianza en Contrapartes

3.9 Autorización de transacciones

3.10 No negación

3.11 Sendero Seguro

3.12 Protección de funciones de seguridad

3.13 Administración de Llaves Criptográficas

3.14 Prevención, Detección y Corrección de Software “Malicioso”

3.15 Arquitectura de *Fire Walls* y conexión a redes públicas

3.16 Protección de Valores Electrónicos

4 Administración de la configuración

4.1 Configuración Base

4.2 Registro de Estatus

4.3 Control de la Configuración

4.4 Software no Autorizado

4.5 Registro de la Configuración

5. Manejo de problemas e incidentes

Sistema de Administración de Problemas

6. Administración de datos

Protección de Información Sensible durante transmisión y transporte

Protección de Mensajes Sensitivos

Autenticación e Integridad

Integridad de Transacciones Electrónicas

Estos objetivos de control se lo ubica en las divisiones que se ha realizado para esta auditoría para que de esta manera sea mas sencillo evaluar desde diferentes perspectivas (Gerencia, red lógica y física) a las redes y comunicaciones.

Gerencia

- Estándares de Tecnología
- Buró de Ayuda.
- Registro de Preguntas del Usuario.
- Registro de la Configuración.
- Identificación, Autenticación y Acceso.
- Revisión Gerencial de Cuentas de Usuario.
- Clasificación de Datos.
- Reportes de Violación y de Actividades de Seguridad.
- Confianza en Contrapartes.
- Autorización de transacciones.
- Sendero Seguro.
- Protección de funciones de seguridad.
- Administración de Llaves Criptográficas.
- Prevención, Detección y Corrección de Software "Malicioso".
- Arquitectura de *Fire Walls* y conexión a redes públicas.
- Protección de Valores Electrónicos.
- Configuración Base.
- Registro de Estatus.

- Control de la Configuración.
- Software no Autorizado.
- Sistema de Administración de Problemas.
- Protección de Información Sensible durante transmisión y transporte.
- Protección de Mensajes Sensitivos.
- Autenticación e Integridad.
- Integridad de Transacciones Electrónicas.

Red Física

- Protección de Información Sensible durante transmisión y transporte.
- Protección de Valores Electrónicos.
- Protección de funciones de seguridad.
- Re acreditación.
- Vigilancia de Seguridad.
- Identificación, Autenticación y Acceso.
- Estándares de Tecnología.

Red Lógica

- Integridad de Transacciones Electrónicas.
- Protección de Mensajes Sensitivos.
- Protección de Información Sensible durante transmisión y transporte.
- Arquitectura de *FireWalls* y conexión a redes públicas.
- Prevención, Detección y Corrección de Software "Malicioso".
- Administración de Llaves Criptográficas.

- Protección de funciones de seguridad.
- Sendero Seguro.
- No negación.
- Autorización de transacciones.
- Re acreditación.
- Vigilancia de Seguridad.
- Seguridad de Acceso a Datos en Línea.
- Identificación, Autenticación y Acceso.
- Estándares de Tecnología.

PROCESO DE AUDITORIA

Se procede a seleccionar los puntos y objetivos de control que permitirán evaluar un área especifica, finalmente se debe dirigir a la capitulo No. 2 en la parte de "Examen detallado de áreas criticas".

CUESTIONARIOS DE AYUDA

CUESTIONARIO No. 1

PREGUNTAS DIRIGIDAS AL JEFE DE LA GERENCIA DE FUNCIONES DE SERVICIOS DE INFORMACIÓN

Objetivos:

- **Conocer los estándares con que cuenta la Armada, así como las áreas donde se tienen.**
- **Conocer las políticas y marcos de referencia con que cuenta la Armada para redes y comunicaciones.**

Marque con una Circulo o "X" la respuesta. Le recordamos que su respuesta esta sujeta a una verificación física y a pruebas. El valor de cada pregunta es de 5 puntos.

1. Marque las áreas en donde existe estándares y el estándar que se usa
    a. Cableado Estructurado.....
    b. Wíreless.....
    c. Enlaces por antena.....
    d. Elementos pasivos de la red.....
    e. Elementos activos de la red.....

1. Se cuenta con políticas organizacionales que instrumenten controles para proporcionar autenticidad de transacciones.

    SI NO

3. Se cuenta con políticas organizacionales que, en donde sea apropiado, las transacciones no puedan ser negadas por ninguna de las partes (origen y destino).

    SI NO

4. Se cuenta con políticas organizacionales en el que la información de transacciones sensitivas es enviada y recibida exclusivamente a través de canales o senderos seguros *(trusted path*s).

    SI NO

5. Se cuentan con políticas de prohibición para introducir programas personales o conectar equipos privados a la red local.

    SI NO

6. Se cuenta con políticas organizacionales que instrumenten prácticas de control para verificar la autenticidad de las contrapartes que proporcionan instrucciones o transacciones electrónicas.

    SI NO

7. Existe un marco de referencia de adecuadas medidas de control preventivas, detectivas y correctivas.

    SI NO

CUESTIONARIO No. 2

PREGUNTAS DIRIGIDAS AL JEFE DE SERVICIOS DE INFORMACIÓN.

Objetivos:

- Verificar la existencia de la función de soporte a usuarios.
- Evaluar el registro de las preguntas del usuario.
- Conocer los aspectos que integran el sistema de administración de problemas.

1. Existen instalaciones reales, divisiones o departamentos que lleven a cabo la función del buró de ayuda al personal en cuanto a redes y comunicaciones.

   SI NO

2. Se establecen procedimientos para registrar todas las preguntas de los usuarios.

   SI NO

3. Cuando las preguntas no puedan ser resueltas inmediatamente se:
   a. Reasignan apropiadamente dentro de la función de servicios de información hasta el nivel adecuado para atenderlas.
   b. Se establecen procedimientos para monitorear oportunamente la atención a las preguntas de los clientes.
   c. Se realiza un análisis de las preguntas, sus repuestas, tiempos de respuesta y la identificación de tendencias

4. Los problemas se registran en un sistema de administración de problemas.

   SI NO

5. El nivel de documentación para las actividades del buró de ayuda es adecuado y actual.

   SI NO

6. Se realiza un análisis de las preguntas, sus repuestas, tiempos de respuesta y la identificación de tendencias.

   SI NO

7. Se cuenta con procedimientos de escalamiento de problemas.

   SI NO

8. El sistema de administración de problemas proporciona elementos adecuados para pistas de auditoria que permitan el seguimiento de las causas a partir de un incidente

SI NO

CUESTIONARIO No. 3

PREGUNTAS DIRIGIDAS AL JEFE DE REDES Y COMUNICACIONES.

Objetivo:

- Verificar que la configuración contemple procedimientos que registren y almacenen la configuraciones base.
- Verificar que se evalúe el desempeño de los servicios técnico de las redes y comunicaciones.
- Evaluar los procedimientos para identificación, autenticación y acceso a la red y equipos de comunicación.

1. Se cuentan con procedimientos para que se registren los elementos de configuración autorizados e identificables en el inventario, al momento de la adquisición.

SI NO

2. Se cuentan con procedimientos para dar seguimientos a los cambios en la configuración .

SI NO

3. Existe una configuración base de elementos como punto de verificación al cual regresar después de las modificaciones.

SI NO

4. Los registros de configuración reflejen el estatus real de todos los elementos de la configuración incluyendo la historia de los cambios

SI NO

5. Se realiza revisiones periódicas del registro de la configuración

SI NO

6. Se realiza el monitoreo y se reporta los alcances de los criterios de desempeño del servicio monitoreado y todos los problemas encontrados.

SI NO

7. Se analizan las estadísticas de monitoreo.

SI NO

8. Se toman acciones correctivas apropiadas y se investigan las fallas.

SI NO

9. Se cuenta con las reglas de acceso a los recursos de la red y de equipos de comunicación.

SI NO

10. Se cuenta con un mecanismo de autenticación de usuarios identificados y recursos asociados con las reglas de acceso.

SI NO

11. Se cuenta con procedimientos de conexión de usuario.

SI NO

12. En elementos activos de la red los accesos para servicio remoto esta inhabilitados.

SI NO

13. El software de comunicaciones para permitir el acceso, exige código de usuarios y contraseña.

SI NO

14. Las claves y contraseñas cuentan con un procedimiento para ser creadas.

SI NO

15. Las claves y contraseñas se cambian periódicamente.

SI NO

16. Se inhabilitaron y / o cambiado las contraseñas y / o claves de acceso en los elementos pasivos y activos de la red, luego de ser instaladas y configuradas.

SI NO

17. Se cuenta con dispositivos / procedimientos de seguridad para impedir acceso no autorizados al sistema informático**.**

SI NO

18. Se tiene procedimientos específicos de control para el uso del servicio remot**o.**

SI NO

19. Las puertas traseras y accesos no especificados están bloqueados.

SI NO

20. Se protege consistentemente la integridad de todas las tarjetas o dispositivos físicos similares, que son utilizados para autenticación o almacenamiento de información financiera u otra información sensitiva.

SI NO

21. Se verifica adecuadamente la autencidad e integridad de información que es originada fuera de la organización .(información recibida por teléfono, correo de voz fax, documentos de papel y correo electrónico.)

SI NO

CUESTIONARIO No. 4

PREGUNTAS DIRIGIDAS AL JEFE DE REDES Y COMUNICACIONES.

Objetivos:

- Evaluar la seguridad en el control, vigilancia, reportes, cuentas de usuario, acceso a datos en línea, diseño, administración de llaves criptográficas, de las redes y comunicaciones

1. Se cuenta con procedimientos acorde con la política de seguridad que garantiza el control de la seguridad de acceso.

SI NO

2. Estos procedimientos toman como base las necesidades individuales de visualizar, agregar, modificar o eliminar datos.

SI NO

3. Existen controles para asegurar que la identificación y los derechos de acceso así como la identidad del sistema y la propiedad de los datos, son establecidos y administrados de forma única y centralizada, para obtener consistencia y eficiencia de un control global de acceso.

SI NO

4. Se revisan controles de seguridad asociados a computadores con módem.

SI NO

5. Se cuenta con un proceso de control establecido para revisar y confirmar periódicamente los derechos de acceso.

SI NO

6. Existen controles para asegurar que la identificación y los derechos de acceso de los usuarios son establecidos y administrados de forma única y centralizada.

   SI NO

7. La actividad de seguridad es registrada.

   SI NO

8. Cualquier indicación sobre una inminente violación de seguridad se notifica inmediatamente al administrador.

   SI NO

9. Cuando se realiza una violación esta es registrada, reportada, revisada y escaladas apropiadamente.

   SI NO

10. Se revisa periódicamente la red de comunicaciones, buscando intercepciones activas o pasivas.

    SI NO

11. Existen procedimientos de registro para capturar y ayudar a reconstruir todas las actividades de las transacciones.

    SI NO

12. Los archivos de registro son revisados diariamente.

    SI NO

13. Existen procedimientos de control sobre la generación e intercambio de claves.

    SI NO

14. Se tiene controles para proporcionar no negación *(non repudiatio*n) de origen o destino, prueba de envío *(proof of submissio*n), y recibo de transacciones.

    SI NO

15. El hardware y software relacionado con seguridad se encuentra protegido contra intromisiones para proteger su integridad y contra divulgación de sus claves secretas.

    SI NO

16. La organización mantiene discreción sobre el diseño de su seguridad, pero no basar la seguridad en mantener el diseño como secreto.

    SI NO

17. Se implementan procedimientos y protocolos a ser utilizados en la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas.

    SI NO

18. Las claves de cifrado son cambiadas regularmente.

SI NO

CUESTIONARIO No. 5

PREGUNTAS DIRIGIDAS AL JEFE DE REDES Y COMUNICACIONES.

Objetivo:

- Verificar que si siga un proceso de acreditación de los equipos de prueba.

1. Se pone a prueba, periódicamente, mediante programas adecuados y actualizados a:
    a. Servidores, desde dentro del servidor.
    b. Servidores, desde la red interna.
    c. Servidores Web.
    d. Intranet.
    e. Firewalls.
2. Los equipos de prueba de comunicaciones usados para resolver los problemas de comunicación de datos tiene propósitos y funciones definidos.

SI **NO**

3. Existen controles adecuados sobre los equipos de prueba de comunicaciones usados.

SI **NO**

CUESTIONARIO No. 6

PREGUNTAS DIRIGIDAS AL JEFE DE REDES Y COMUNICACIONES.

Objetivos:

- Verificar que la arquitectura de comunicaciones utilice diferentes rutas de transmisión.
- Verificar que se utilice cifrado de información.
- Evaluar el funcionamiento básico del firewall.

1. Utiliza indistintamente cualquier ruta disponible de transmisión.

SI NO

2. Al usar canales de comunicación entre edificios. Estos canales se cifran automáticamente.

   SI NO

3. Se cuenta con sistemas *FireWall* adecuados para proteger la negación de servicios y cualquier acceso no autorizado a los recursos internos

   SI NO

CUESTIONARIO No. 7

PREGUNTAS DIRIGIDAS AL JEFE DE REDES Y COMUNICACIONES.

Objetivos:

- Evaluar la protección de la información sensible durante la transmisión y transporte.
- Evaluar la protección de mensajes sensitivos y la integridad de las transacciones electrónicas.

1. La transmisión y transporte de la información sensible, tiene una adecuada protección contra acceso o modificación no autorizada, así como contra envíos a direcciones erróneas.

   SI NO

2. Que tipo de protección es

.....

.....

3. Tiene procedimientos y protocolos ha ser utilizados para el aseguramiento de la integridad, confidencialidad y no negación de mensajes sensitivos.

   SI NO

4. Existen análisis de riesgos para las aplicaciones de proceso de datos a fin de identificar aquellas en las que el cifrado resulte apropiado.

   SI NO

5. La información que se envía por el Internet cuenta con cifrado.

   SI NO

6. Los mensajes lógicos transmitidos identifican el originante, la fecha, la hora y el receptor.

   SI NO

7. El software de comunicaciones ejecuta procedimientos de control y correctivos ante mensajes duplicados, fuera de orden, perdidos o retrasados.

SI NO

8. Se implementa procedimientos y prácticas para transacciones electrónicas que sean sensitivas y críticas para la Organización.

SI NO

9. Se asegura la integridad y autencidad de:
    a. Atomicidad.
    b. Consistencia
    c. Aislamiento
    d. durabilidad

al momento de realizar transacciones electrónicas.

10. Existen controles para que los datos sensibles solo puedan ser impresos en las impresoras designadas y vistos desde los terminales autorizados.

SI NO

AUDITORIA INFORMATICA PARA SOFTWARE EN EXPLOTACION

INTRODUCCIÓN

El nivel de competencia que existe, hoy en día, entre las empresas les obliga a tomar decisiones rápidas y acertadas. Es necesario, para ello, el funcionamiento adecuado de los sistemas informáticos y su continua actualización. De esta forma, es decir, combinando esas tecnologías con una adecuada organización y una gestión eficiente, las empresas podrán alcanzar sus objetivos de manera satisfactoria.

Este capítulo pretende elaborar el esquema de un procedimiento para llevar a cabo las auditorías de explotación de los sistemas de información siguiendo la clasificación de los controles que hace el Proyecto COBIT.

OBJETIVOS

- Auditar la definición de la Arquitectura de Información.
- Auditar la determinación de la dirección tecnológica.
- Auditar la definición de la organización y de las relaciones de TI.
- Auditar la comunicación de la dirección y aspiraciones de la gerencia.
- Auditar la administración de recursos humanos.
- Auditar la identificación de Soluciones.
- Auditar la adquisición y mantenimiento de arquitectura de software.

- Auditar el desarrollo y mantenimiento de procedimientos relacionados con tecnología de información.
- Auditar la instalación y acreditación de sistemas.
- Auditar la administración de cambios.
- Auditar la definición de niveles de servicio.
- Auditar la administración de servicios prestados por terceros.
- Auditar la seguridad de sistemas.
- Auditar la educación y entrenamiento de usuarios.
- Auditar el apoyo y asistencia a los clientes de tecnología de Información.
- Auditar la administración de la Configuración.
- Auditar la administración de problemas e incidentes.
- Auditar la administración de Datos.
- Auditar la administración de instalaciones.
- Auditar la administración de Operaciones.

ALCANCE

En un sentido amplio se puede considerar un Sistema de Información como un conjunto de componentes que interactúan para que la empresa pueda alcanzar sus objetivos satisfactoriamente, por lo mencionado anteriormente, a un sistema de información se lo puede dividir en:

Datos.

- Entrada: Es toda la información que se ingresa al sistema de manera manual o automática.
- Salida: Información procesada.

Aplicaciones.

- Cliente-Servidor: La computación cliente-servidor es un intento de equilibrar el proceso de una red hasta que se comparta la potencia de procesamiento entre computadores que llevan a cabo servicios especializados tales como acceder a bases de datos y aquellos que llevan a cabo tareas tales como la visualización IGU (Interfaz Gráfica de Usuario) que es más adecuado para el punto final dentro de la red.
- A n capas: Una arquitectura de dos capas consiste en una capa de lógica y presentación, y otra capa de base de datos. La primera tiene que ver con presentar al usuario conjuntos de objetos visuales y llevar a cabo el procesamiento que requieren los datos producidos por el usuario y los devueltos por el servidor.

Instalaciones. El proceso de instalación.

Personal. Personal que interactúa con el sistema.

MARCO TEÓRICO

Importancia del Software.

"El software de computadora es una de las pocas tecnologías clave que tendrá un impacto significativo en los años 90. Se trata de un mecanismo para automatizar negocios,

industrias y gobiernos, un medio de transferir nuevas tecnologías, un método para adquirir experiencia valiosa que otras personas puedan utilizar, un medio para diferenciar los productos de una compañía de los productos de sus competidores, y una ventana que permite examinar el conocimiento colectivo de una corporación. El software es crucial para casi todos los aspectos del negocio. Pero de muchas maneras, el software es también una tecnología oculta. Encontramos el software cuando nos desplazamos hasta nuestro trabajo, cuando efectuamos cualquier compra, cuando nos detenemos en el banco, cuando hacemos una llamada telefónica, cuando visitamos al médico o cuando realizamos cualquiera de los cientos de actividades diarias que reflejan la vida moderna.

El software está en todas partes y, sin embargo, hay muchas personas en puestos de responsabilidad que tienen poca o ninguna comprensión de lo que realmente es, como se construye, o de lo que significa para las instituciones que lo controlan. Y, lo que es más importante, tienen muy poca idea de los peligros y oportunidades que este software ofrece".[7]

El ámbito del cambio

Los cambios en la informática durante los últimos 50 años han sido controlados por los avances en las ciencias experimentales duras (física, química, ciencia de materiales e ingeniería). Durante la próxima década, los avances revolucionarios en la informática serán dirigidos por las ciencias no experimentales suaves (psicología humana, biología, neurofisiología, sociología, filosofía y otras). El período de gestación de las tecnologías informáticas que se puede derivar de estas disciplinas es muy difícil de predecir.

[7] Pressman, Roger, **INGENIERÍA DEL SOFTWARE UN ENFOQUE PRÁCTICO**, Mc Graw Hill, Quinta Edición, Página 574

Es posible que la influencia de las ciencias no experimentales ayude a modelar la dirección de la investigación informática en las ciencias experimentales.

Los cambios que afectarán a la ingeniería del software durante la próxima década se verán influenciados por cuatro fuentes simultáneas: las personas que realizan el trabajo; el proceso que aplican; la naturaleza de la información, y la tecnología informática subyacente.

Nuevos modos de representar la información.

A lo largo de las dos últimas décadas, se ha producido una sutil transición en la terminología que se utiliza para describir el trabajo de desarrollo de software realizado para la comunidad de negocios. Hace treinta años, el término procesamiento de datos era la frase operativa para describir la utilización de computadoras en un contexto de negocio. En la actualidad, el proceso de datos ha dado lugar a otra frase "tecnología de la información" que significa lo mismo pero presenta un sutil cambio de nuestro centro de atención. La importancia ya no está meramente en procesar grandes cantidades de datos, sino más bien en extraer una información significativa a partir de estos datos.

Cuando en la actualidad se describen las aplicaciones de software, las palabras datos e información aparecen en numerosas ocasiones. La palabra conocimiento se encuentra en algunas aplicaciones de inteligencia artificial, pero su utilización es relativamente escasa. Casi nadie describe la sabiduría en el contexto de las aplicaciones del software para computadoras.

Los datos son información pura, una colección de hechos que es preciso procesar para que sean significativos. La información se deriva asociando los hechos en el seno de un contexto dado. El conocimiento asocia la información obtenida en un contexto con otra información obtenida en un contexto con otra información obtenida en un contexto distinto. Por último la sabiduría se produce cuando se derivan unos principios generalizados de conocimientos dispares.

Visión general de la ingeniería del software.

La ingeniería es el análisis, diseño, construcción, verificación y gestión de entidades técnicas, con independencia de la entidad a la que se va a aplicar ingeniería.

Para construir la ingeniería del software adecuadamente, se debe definir un proceso de desarrollo de software. El trabajo que se asocia a la ingeniería del software se puede dividir en tres fases genéricas, con independencia del área de aplicación, tamaño o complejidad del proyecto.

La fase de definición se centra sobre el qué. Es decir, durante la definición, el que desarrolla el software intenta identificar qué información ha de ser procesada, qué función y rendimiento se desea, qué comportamiento del sistema, qué interfases van a ser establecidas, qué restricciones de diseño existen, y qué criterios de validación se necesita paran para definir un sistema correcto.

La fase de desarrollo se centra en el cómo. Es decir, durante el desarrollo un ingeniero del software intenta definir cómo han de diseñarse las estructuras de datos, como ha de

implementarse la función dentro de una arquitectura de software, cómo han de implementarse los detalles procedimentales, cómo han de caracterizarse interfases, cómo ha de traducirse el diseño en un lenguaje de programación y cómo ha de realizarse la prueba.

La fase de mantenimiento se centra en el cambio que va asociado a la corrección de errores, a las adaptaciones requeridas a medida que evoluciona el entorno del software y a cambios debidos a las mejoras producidas por los requisitos cambiantes del cliente.

Proceso, métodos y herramientas.

La ingeniería del software es una tecnología multicapa. Cualquier enfoque de ingeniería debe apoyarse sobre un compromiso de organización de calidad. El fundamento de la ingeniería del software es la capa de proceso. El proceso de la ingeniería del software es la unión que mantiene juntas las capas de tecnología y que permiten un desarrollo racional y oportuno de la ingeniería del software. El proceso define un marco de trabajo para un conjunto de áreas clave de proceso que se deben establecer para la entrega efectiva de la tecnología de la ingeniería del software.

Los métodos de la ingeniería del software indican cómo construir técnicamente el software. Los métodos abarcan una gran gama de tareas que incluyen análisis de requisitos, diseño, construcción de programas, pruebas y mantenimiento.

Las herramientas de la ingeniería del software proporcionan un enfoque automático o semi-automático para el proceso y para los métodos. Cuando se integran herramientas para que la información creada por una herramienta la pueda utilizar otra, se establece un sistema

de soporte para el desarrollo del software llamado ingeniería del software asistida por computadora.

Categorías de servidores.

Ya se han desarrollado una gran variedad de servidores, a continuación se mencionan algunos:

Servidores de archivos. Un servidor de archivos proporciona archivos para clientes. Estos servidores se utilizan todavía en algunas aplicaciones donde los clientes requieren un procesamiento complicado fuera del rango normal de procesamiento que se puede encontrar en bases de datos comerciales.

Servidores de bases de datos. Los servidores de bases de datos son computadoras que almacenan grandes colecciones de datos estructurados.

Servidores de software de grupo. Software de grupo es el término que se utiliza para describir el software que organiza el trabajo de un grupo de trabajadores.

Servidores Web. Los documentos Web se almacenan como páginas en una computadora conocida como servidor Web.

Servidores de correo. Un servidor de correo gestiona el envío y recepción de correo de un grupo de usuarios.

Servidores de objetos. Uno de los desarrollos más excitantes en la informática distribuida durante los últimos años ha sido el avance realizado, tanto por parte de los desarrolladores, como por parte de los investigadores, para proporcionar objetos distribuidos. Un servidor que contiene objetos que puedan accederse a distancia se conoce como servidor de objetos.

Servidores de impresión. Los servidores de impresión dan servicio a las solicitudes de un cliente remoto.

Servidores de aplicaciones. Un servidor de aplicaciones se dedica a una aplicación única.

Diseño de la Interfaz de Usuario.

El proceso global para el diseño de la interfaz de usuario comienza con la creación de diferentes modelos de funcionamiento del sistema. Es entonces cuando se determinan las tareas orientadas al hombre y a la máquina que se requieren para lograr el funcionamiento del sistema.

Modelo de diseño de la interfaz.

Cuando se va a diseñar la interfaz de usuario entran en juego cuatro modelos diferentes. El ingeniero del software crea un modelo de diseño; cualquier otro ingeniero establece un modelo de usuario, el usuario final desarrolla una imagen mental que se suele llamar modelo de usuario, y los que implementan el sistema crean una imagen de sistema.

Un modelo de diseño de un sistema completo incorpora las representaciones del software en función de los datos, arquitectura, interfaz, y procedimiento.

El modelo de usuario representa el perfil de los usuarios finales del sistema.

El modelo de usuario es la imagen del sistema que el usuario final tiene en su mente.

La imagen del sistema es una combinación de fachada externa del sistema basado en computadora y la información de soporte todo lo cual ayuda a describir la sintaxis y la semántica del sistema.

Categorías de Usuarios.

Principiantes. En general no tienen conocimientos sintácticos ni conocimientos semánticos de la utilización de la aplicación o del sistema.

Usuarios esporádicos y con conocimiento. Poseen un conocimiento semántico razonable, pero una retención baja de la información necesaria para utilizar la interfaz.

Usuarios frecuentes y con conocimientos. Poseen el conocimiento sintáctico y semántico suficiente como para llegar al síndrome del usuario avanzado, esto es, individuos que buscan interrupciones breves y modos abreviados de interacción.

PUNTOS DE CONTROL

Los puntos de control para esta auditoria son:

1. Definición de la Arquitectura de Información.
2. Determinación de la dirección tecnológica.
3. Definición de la organización y de las relaciones de TI.
4. Comunicación de la dirección y aspiraciones de la gerencia.
5. Administración de recursos humanos.
6. Identificación de Soluciones.
7. Adquisición y mantenimiento de arquitectura de software.

8. Desarrollo y mantenimiento de procedimientos relacionados con tecnología de información.
9. Instalación y acreditación de sistemas.
10. Administración de cambios.
11. Definición de niveles de servicio.
12. Administración de servicios prestados por terceros.
13. Garantizar la seguridad de sistemas.
14. Educación y entrenamiento de usuarios.
15. Apoyo y asistencia a los clientes de tecnología de Información.
16. Administración de la Configuración.
17. Administración de problemas e incidentes.
18. Administración de Datos.
19. Administración de instalaciones.
20. Administración de Operaciones.

Estos puntos de control permiten:

- Organizar de la mejor manera los sistemas de información.
- Aprovechar la tecnología disponible o tecnología emergente.
- Prestación de servicios de TI.
- Asegurar el conocimiento y comprensión del usuario sobre dichas aspiraciones.
- Maximizar las contribuciones del personal a los procesos de TI.
- Cumplir con obligaciones legales, regulatorias y contractuales.
- Asegurar el mejor enfoque para cumplir con los requerimientos del usuario.

- Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios.
- Asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas.
- Verificar y confirmar que la solución sea adecuada para el propósito deseado.
- Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores.
- Establecer una comprensión común del nivel de servicio requerido.
- Asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos.
- Mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones.
- Salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida.
- Asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados.
- Asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente.
- 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.
- Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir cualquier recurrencia.
- Asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento.
- Proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales o fallas humanas.

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

Además se debe tomar en cuenta ciertos lineamientos para una mejor evaluación de los puntos de control:

- Documentación.
- Diccionario de datos.
- Reglas de sintaxis de datos.
- Monitoreo de desarrollos tecnológicos.
- Contingencias.
- Planes de adquisición.
- Propiedad, custodia.
- Segregación de funciones.
- Roles y responsabilidades.
- Directrices tecnológicas.
- Políticas de seguridad.
- Políticas de control interno.
- Capacitación.
- Desarrollo de conciencia.
- Entrenamiento cruzado.
- Procedimientos de acreditación.
- Leyes, regulaciones, contratos.
- Seguridad y ergonomía.

- Estudios de factibilidad.
- Arquitectura de información.
- Pistas de auditoría.
- Evaluación de tecnología.
- Seguridad del software de sistema, instalación, mantenimiento y control sobre cambios.
- Procedimientos y controles de usuarios.
- Procedimientos y controles operacionales.
- Materiales de entrenamiento.
- Capacitación.
- Conversión/carga de datos.
- Garantías de integridad.
- Respaldo y recuperación.
- Pruebas y entrenamiento sistemáticos y regulares.
- Acceso.
- Perfiles e identificación de usuarios.
- Administración de llaves criptográficas.
- Manejo, reporte y seguimiento de incidentes.
- Consultas de usuarios y respuesta a problemas.
- Registro de activos.
- Administración de cambios en la configuración.
- Chequeo de software no autorizado.
- Controles de almacenamiento de software.
- Suficientes pistas de auditoría de problemas y soluciones.

- Resolución oportuna de problemas reportados.
- Reportes de incidentes.
- Controles de entrada.
- Controles de procesamiento.
- Controles de salida.
- Identificación, movimiento y administración de la librería de medios.
- Administración de almacenamiento y respaldo de medios.
- Autenticación e integridad.
- Identificación del centro de cómputo.
- Seguridad física.
- Protección contra amenazas ambientales.
- Manual de procedimiento de operaciones.
- Documentación de procedimientos de arranque.
- Registro de eventos de sistemas.

Puntos y objetivos de Control.

1 Definición de la Arquitectura de Información

1.1 Modelo de la Arquitectura de Información

1.2 Diccionario de Datos y Reglas de Sintaxis de Datos de la Corporación

1.3 Esquema de Clasificación de Datos

1.4 Niveles de Seguridad

2 Determinación de la dirección tecnológica

2.1 Planes de Adquisición de Hardware y Software

2.2 Estándares de Tecnología

3 Definición de la organización y de las relaciones de TI

3.1 Responsabilidad de la Seguridad Lógica y Física

3.2 Propiedad y Custodia

3.3 Propiedad de Datos y Sistemas

3.4 Segregación de Funciones

4 Comunicación de la dirección y aspiraciones de la gerencia

4.1 Cumplimiento de Políticas, Procedimientos y Estándares

5 Administración de recursos humanos

5.1 Entrenamiento de Personal

6 Aseguramiento del cumplimiento de requerimientos externos

6.1 Privacidad, propiedad intelectual y flujos de datos y Flujo de Datos

7 Identificación de Soluciones

7.1 Adquisición de Productos de Software

7.2 Mantenimiento de Software de Terceras Partes

7.3 Contratos de Programación de Aplicaciones

8 Adquisición y mantenimiento de arquitectura de software

12 Definición de niveles de servicio

- 12.1 Monitoreo y Reporte
- 12.2 Revisión de Convenios y Contratos de Nivel de Servicio

13 Administración de servicios prestados por terceros

- 13.1 Interfases con Proveedores
- 13.2 Relaciones de Dueños
- 13.3 Contratos con Terceros
- 13.4 Calificación de Terceros
- 13.5 Contratos con Fuentes Externas
- 13.6 Continuidad de Servicios
- 13.7 Monitoreo

14 Garantizar la seguridad de sistemas

- 14.1 Contenido del Plan de Continuidad de Tecnología de Información
- 14.2 Mantenimiento Plan de Continuidad de Tecnología de Información
- 14.3 Capacitación sobre el Plan de Continuidad de Tecnología de Información
- 14.4 Procedimientos de respaldo de procesamiento para Departamentos usuarios
- 14.5 Recursos Críticos de Tecnología de Información
- 14.6 Centro de cómputo y Hardware de Respaldo

15 Garantizar la seguridad de sistemas

- 15.1 Administrar Medidas de Seguridad
- 15.2 Identificación, Autenticación y Acceso

15.3 Seguridad de Acceso a Datos en Línea

15.4 Administración de Cuentas de Usuario

15.5 Revisión Gerencial de Cuentas de Usuario

15.6 Control de Usuarios sobre Cuentas de Usuario

15.7 Vigilancia de Seguridad

15.10 Reportes de Violación y de Actividades de Seguridad

15.11 Manejo de Incidentes

15.14 Autorización de transacciones

15.17 Protección de funciones de seguridad

15.18 Administración de Llaves Criptográficas

15.19 Prevención, Detección y Corrección de Software "Malicioso"

16 Educación y entrenamiento de usuarios

16.1 Identificación de Necesidades de Entrenamiento

16.2 Organización del Entrenamiento

16.3 Entrenamiento sobre Principios y Conciencia de Seguridad

17 Apoyo y asistencia a los clientes de tecnología de Información

17.1 Buró de Ayuda

17.2 Registro de Preguntas del Usuario

17.3 Escalamiento de Preguntas del Cliente

17.4 Análisis y Reporte de Tendencias

18 Administración de la Configuración

18.1 Registro de la Configuración

18.2 Configuración Base

18.3 Registro de Estatus

18.4 Almacenamiento de Software

19 Administración de problemas e incidentes.

19.1 Seguimiento de Problemas y Pistas de Auditoría

20 Administración de Datos.

20.1 Procedimientos de Preparación de Datos

20.2 Procedimientos de Autorización de Documentos Fuente

20.3 Recopilación de Datos de Documentos Fuente

20.4 Manejo de errores de documentos fuente

20.5 Retención de Documentos Fuente

20.6 Procedimientos de Autorización de Entrada de Datos

20.7 Chequeos de Exactitud, Suficiencia y Autorización

20.8 Manejo de Errores en la Entrada de Datos

20.9 Integridad de Procesamiento de Datos

20.10 Validación y Edición de Procesamiento de Datos

20.11 Manejo de Errores en el Procesamiento de Datos

20.12 Manejo y Retención de Datos de Salida

20.13 Distribución de Datos de Salida

20.14 Balanceo y Conciliación de Datos de Salida

20.15 Revisión de Datos de Salida y Manejo de Errores

22.4 Salidas de la Calendarización de Trabajos Estándar

22.5 Continuidad de Procesamiento

22.6 Bitácoras de Operación

22.7 Operaciones Remotas

Estos objetivos de control se los ubica en las divisiones que se ha realizado para esta auditoría para que de esta manera sea más sencillo evaluar desde diferentes perspectivas (Datos, Aplicaciones, Instalaciones, Personal) al software en explotación.

Datos.

- Modelo de la Arquitectura de Información
- Diccionario de Datos y Reglas de Sintaxis de Datos de la Corporación
- Esquema de Clasificación de Datos
- Niveles de Seguridad
- Propiedad y Custodia
- Propiedad de Datos y Sistemas
- Segregación de Funciones
- Privacidad, propiedad intelectual y flujos de datos y Flujo de Datos
- Identificación, Autenticación y Acceso
- Seguridad de Acceso a Datos en Línea
- Vigilancia de Seguridad
- Autorización de transacciones
- Protección de funciones de seguridad

- Administración de Llaves Criptográficas
- Prevención, Detección y Corrección de Software “Malicioso”
- Procedimientos de Preparación de Datos
- Procedimientos de Autorización de Documentos Fuente
- Recopilación de Datos de Documentos Fuente
- Manejo de errores de documentos fuente
- Retención de Documentos Fuente
- Procedimientos de Autorización de Entrada de Datos
- Chequeos de Exactitud, Suficiencia y Autorización
- Manejo de Errores en la Entrada de Datos
- Integridad de Procesamiento de Datos
- Validación y Edición de Procesamiento de Datos
- Manejo de Errores en el Procesamiento de Datos
- Manejo y Retención de Datos de Salida
- Distribución de Datos de Salida
- Balanceo y Conciliación de Datos de Salida
- Revisión de Datos de Salida y Manejo de Errores
- Provisiones de Seguridad para Reportes de Salida
- Protección de Información Sensible durante transmisión y transporte
- Administración de Almacenamiento
- Períodos de Retención y Términos de Almacenamiento
- Sistema de Administración de la Librería de Medios
- Responsabilidades de la Administración de la Librería de Medios
- Respaldo y Restauración

- Funciones de Respaldo
- Almacenamiento de Respaldos
- Archivo
- Protección de Mensajes Sensitivos
- Autenticación e Integridad
- Integridad Continua de Datos Almacenados

Aplicaciones.

- Planes de Adquisición de Hardware y Software
- Estándares de Tecnología
- Responsabilidad de la Seguridad Lógica y Física
- Adquisición de Productos de Software
- Mantenimiento de Software de Terceras Partes
- Contratos de Programación de Aplicaciones
- Evaluación de Nuevo Hardware y Software
- Mantenimiento Preventivo para Hardware
- Evaluación del Impacto
- Control de Cambios
- Política de Liberación de Software
- Distribución de Software
- Monitoreo y Reporte
- Revisión de Convenios y Contratos de Nivel de Servicio
- Interfases con Proveedores

- Relaciones de Dueños
- Contratos con Terceros
- Calificación de Terceros
- Contratos con Fuentes Externas
- Continuidad de Servicios
- Monitoreo
- Contenido del Plan de Continuidad de Tecnología de Información
- Mantenimiento Plan de Continuidad de Tecnología de Información
- Procedimientos de respaldo de procesamiento para Departamentos usuarios
- Recursos Críticos de Tecnología de Información
- Centro de cómputo y Hardware de Respaldo
- Administrar Medidas de Seguridad
- Almacenamiento de Software
- Seguimiento de Problemas y Pistas de Auditoría
- Seguridad Física
- Discreción de las Instalaciones de Tecnología de Información
- Protección contra Factores Ambientales
- Suministro Ininterrumpido de Energía
- Manual de procedimientos de Operación e Instrucciones
- Documentación del Proceso de Inicio y de Otras Operaciones
- Calendarización de Trabajos
- Salidas de la Calendarización de Trabajos Estándar
- Continuidad de Procesamiento
- Bitácoras de Operación

- Operaciones Remotas

Instalaciones.

- Seguridad del Software del Sistema
- Instalación del Software del Sistema
- Mantenimiento del Software del Sistema
- Paso a Producción
- Mantenimiento Autorizado
- Reportes de Violación y de Actividades de Seguridad
- Manejo de Incidentes
- Registro de la Configuración
- Configuración Base
- Registro de Estatus

Personal.

- Cumplimiento de Políticas, Procedimientos y Estándares
- Entrenamiento de Personal
- Manual de Procedimientos para Usuario
- Manual de Operaciones
- Material de Entrenamiento
- Entrenamiento
- Evaluación de la Satisfacción de los Requerimientos del Usuario

- Documentación y Procedimientos
- Capacitación sobre el Plan de Continuidad de Tecnología de Información
- Administración de Cuentas de Usuario
- Revisión Gerencial de Cuentas de Usuario
- Control de Usuarios sobre Cuentas de Usuario
- Identificación de Necesidades de Entrenamiento
- Organización del Entrenamiento
- Entrenamiento sobre Principios y Conciencia de Seguridad
- Buró de Ayuda
- Registro de Preguntas del Usuario
- Escalamiento de Preguntas del Cliente
- Análisis y Reporte de Tendencias

PROCESO DE AUDITORIA

Se procede a seleccionar los puntos y objetivos de control que permitirán evaluar un área especifica, finalmente se debe dirigir a la capitulo No. 2 en la parte de "Examen detallado de áreas criticas".

CUESTIONARIOS DE AYUDA

CUESTIONARIO No. 1

PREGUNTAS DIRIGIDAS AL JEFE DEL CETEIN

Objetivo:

- Conocer información a cerca del modelo de la arquitectura de información.

- Conocer estándares de la sintaxis de datos.
- Conocer información del diccionario de datos.
- Conocer información de las categorías de seguridad de la información.
- Conocer información de los niveles de seguridad.
- Conocer asignaciones de propiedad y custodia.
- Conocer asignaciones de propiedad.
- Verificar la preparación de datos.
- Verificar la exactitud, suficiencia y autorización de los datos.

1. El modelo de la arquitectura de información es creado por el CETEIN.

   SI NO

2. El modelo de la arquitectura de información es actualizado por el CETEIN.

   SI NO

3. Cada que tiempo se actualiza este modelo.

   ……..

4. Quien aprueba la creación de este modelo.

   ……..

5. Existe algún estándar para las reglas de sintaxis de datos.

   SI NO

6. Existe un diccionario de datos corporativo.

   SI NO

7. Están definidas categorías de seguridad para la información.

   SI NO

8. Están Documentadas estas categorías.

   SI NO

9. Estas categorías tienen propietarios.

   SI NO

10. Existen perfiles de acceso a los datos según la categoría de seguridad.

    SI NO

11. Existen niveles de seguridad para cada clasificación de datos.

    SI NO

12. Se asignan propietarios y custodios de los datos.

SI NO

13. Se asignan propietarios para los activos de información.

SI NO

14. La clasificación de los datos permite conocer los datos que necesitan de protección y no protección.

SI NO

15. Marque las responsabilidades de los propietarios.

- Dar derechos de acceso a los usuarios.
- Dictar medidas de seguridad apropiadas.
- Nombran personal encargados de verificar que las medidas de seguridad se cumplan.

CUESTIONARIO No. 2

PREGUNTAS DIRIGIDAS AL JEFE DEL CETEIN

Objetivo:

- Conocer información del plan de infraestructura tecnológica.
- Conocer información del plan de adquisición de hardware y software.
- Conocer información de los estándares de tecnología.

1. Existe un plan de infraestructura tecnológica.

SI NO

2. Este plan contiene aspectos de contingencias.

SI NO

3. Existen planes de adquisición de hardware y software.

SI NO

4. Existen estándares de tecnología.

SI NO

5. Marque las áreas en las que se cuenta con estándares.

- Definición de variables.
- Documentación.

- Definición de formularios.
- Definición de objetos.
- Definición de paginas html.
- Definición de imágenes.
- Definición de funciones.
- Definición de procedimientos almacenados.
- Definición de tablas.
- Definición de campos.
- Definición de la relaciones.

CUESTIONARIO No. 3

PREGUNTAS DIRIGIDAS AL JEFE DE LA DIVISION DE DESARROLLO DE SISTEMAS

Objetivo:

- Confirmar la implementación del modelo de la arquitectura de información.
- Confirmar la implementación del diccionario de datos y regla de sintaxis.
- Confirmar la implementación del esquema de clasificación de datos.
- Confirmar la implementación de los niveles de seguridad.
- Confirmar la implementación de la propiedad y custodia.
- Confirmar la implementación de la propiedad de datos y sistemas.

1. Se implementa el modelo de la arquitectura de información.

   SI NO

2. Quien actualiza el diccionario de datos corporativo.

   ……..

3. Se implementa las reglas de sintaxis de datos.

   SI NO

4. Se implementa la clasificación de datos.

   SI NO

5. Se implementa los niveles de seguridad para cada clasificación de datos.

SI NO

6. Se mantiene los niveles de seguridad para cada clasificación de datos.

SI NO

7. A través de los niveles de seguridad se puede controlar el acceso a los datos.

SI NO

8. Quien asigna al propietarios y custodio de los datos.

……..

9. Estos propietarios cuentan con funciones y responsabilidades.

SI NO

10. Existen procedimientos de preparación de datos a ser seguidos por los departamentos usuarios.

SI NO

11. El diseño de formas de entrada de datos ayuda a minimizar errores y omisiones.

SI NO

12. Existen procedimientos para manejo de errores.

13. Los datos sobre transacciones, capturados para su procesamiento cuentan con controles para verificar su exactitud, suficiencia y validez.

SI NO

14. Existen procedimientos que aseguran que los datos de entrada sean validados y editados tan cerca del punto de origen como sea posible.

SI NO

CUESTIONARIO No. 4

PREGUNTAS DIRIGIDAS AL JEFE DE LA DIVISION DE DESARROLLO DE SISTEMAS

Objetivo:

- Conocer el funcionamiento de las aplicaciones en base al software que utilizan.
- Confirmar la aplicación de los estándares.

1. La adquisición de hardware satisface las necesidades del software en explotación.

SI NO

2. La adquisición software satisface las expectativas creadas sobre él.

SI NO

3. Los recursos materiales planteados en los planes fueron entregados en los tiempos establecidos.

SI NO

4. Se cumplen con los estándares de tecnología establecidos.

SI NO

CUESTIONARIO No. 5

PREGUNTAS DIRIGIDAS AL JEFE DEL CETEIN

Objetivo:

- Conocer información a cerca de las funciones y responsabilidades del personal.
- Evaluar la supervisión de funciones y responsabilidades.
- Conocer procedimientos de identificación del personal clave.

1. Se define funciones y responsabilidades del personal que va ha interactuar con el sistema de información. Estas funciones y responsabilidades se las actualiza regularmente.

SI NO

2. El personal conoce las funciones y responsabilidades en relación con los sistemas de información.

SI NO

3. Cuando el personal es contratado se establece normas para controlar sus actividades.

SI NO

4. Se supervisa que las funciones y responsabilidades se cumplan a cabalidad.

SI NO

5. Se evalúa si el personal cuenta con autoridad suficiente para realizar sus funciones y cumplir con sus responsabilidades.

SI NO

6. Marque las segregaciones que existen.

- Uso de sistemas de información.
- Entrada de datos.
- Administración de redes.
- Administración de sistemas.
- Administración de cambios.
- Administración de seguridad.

7. Existe una identificación del personal clave en la administración y manejo del sistema.

SI NO

CUESTIONARIO No. 6

PREGUNTAS DIRIGIDAS AL JEFE DE LA DIVISION DE DESARROLLO DE SISTEMAS

Objetivo:

- Verificar que el personal cuente con los accesos necesarios para cumplir con sus funciones.

1. El personal cuenta con los accesos necesarios, al sistema, para que se realice las funciones y responsabilidades a él encomendadas.

SI NO

2. Estas funciones y responsabilidades se cumplen.

SI NO

CUESTIONARIO No. 7

PREGUNTAS DIRIGIDAS AL JEFE DEL CETEIN

Objetivo:

- Conocer información de la calidad del software

1. Existen políticas y procedimientos de aseguramiento de calidad.

   SI NO

2. Cuales son estas políticas y procedimientos de aseguramiento de calidad.

   ……..

3. Que áreas cubren estas políticas y procedimientos de aseguramiento de la calidad.

   ……..

4. Existe un grupo de aseguramiento de la calidad.

   SI NO

5. Quien conforma este grupo.

   ……..

6. El grupo de aseguramiento de la calidad cumple con las tareas a ellos encomendadas.

   SI NO

CUESTIONARIO No. 8

PREGUNTAS DIRIGIDAS AL JEFE DE LA DIVISION DE DESARROLLO DE SISTEMAS

Objetivo:

- Confirmar el cumplimiento de políticas, procedimientos y estándares.

1. Marque las áreas en las que se tiene políticas y procedimientos.
   - Seguridades.
   - Administración del sistema de información.
   - Interacción entre el usuario y el sistema de información.
   - Situaciones Específicas.

2. Existe un control del cumplimiento de Políticas y Procedimientos.

SI NO

CUESTIONARIO No. 9

PREGUNTAS DIRIGIDAS A LOS USUARIOS

Objetivo:

- Verificar el cumplimiento de políticas, procedimientos y estándares.
- Verificar la capacitación del personal

1. Cumple con las políticas y procedimientos establecidos para seguridad.

   SI NO

2. Fue capacitado adecuadamente para el manejo del sistema.

   SI NO

3. Califique la capacitación que recibió.
   - Buena.
   - Regular.
   - Mala.
4. Los documentos fuente autorizados son completos, precisos, registrados apropiadamente y transmitidos oportunamente para el ingreso de datos.

   SI NO

5. Se cuenta con un manual de procedimientos para usuarios.

   SI NO

CUESTIONARIO No. 10

PREGUNTAS DIRIGIDAS AL JEFE DEL CETEIN

Objetivo:

- Conocer información a cerca del plan de pruebas.
- Conocer información a cerca del plan de revisión post-implementación.

- Conocer información a cerca de pruebas piloto/en paralelo.
- Verificar la existencia de documentación de las pruebas del sistema.

1. Existe un plan de pruebas.

   SI NO

2. Los reportes obligatorios identificados en el plan de prueba han sido producidos.

   SI NO

3. Existe un plan de revisión post - implementación para cada sistema de información.

   SI NO

4. Los resultados completos de las pruebas de programas y sistemas son revisados y retenidos para pruebas futuras.

   SI NO

5. Existe documentación de los resultados de las pruebas del sistema.

   SI NO

CUESTIONARIO No. 11

PREGUNTAS DIRIGIDAS AL JEFE DE LA DIVISION DE DESARROLLO DE SISTEMAS

Objetivo:

- Conocer información a cerca del diseño de pistas de auditoría.
- Conocer información de las especificaciones de programas.
- Conocer información de la interfase usuario-máquina.
- Verificar la Controlabilidad del software.
- Verificar la seguridad del software del sistema.
- Conocer información del manual de operaciones.
- Verificar el desempeño del software de aplicación.
- Conocer si existe una conversión de datos.
- Verificar la existencia de documentación y procedimientos.
- Verificar la existencia de un buró de ayuda.

1. Existen mecanismos adecuados para pistas de auditoria en el sistema de información.

SI NO

2. La metodología del ciclo de vida de desarrollo de sistemas requiere la preparación de especificaciones detalladas por escrito de los sistemas de información ha ser modificados.

SI NO

3. La interfase entre el usuario y la máquina es fácil de utilización.

SI NO

4. Existen funciones de ayuda en línea.

SI NO

5. Se cuenta con controles de aplicación que garanticen que los datos de entrada y salida estén completos, así como su precisión, oportunidad y autorización.

SI NO

6. Al concluir el proceso de instalación del software se verifica que no existan puertos abiertos que permitan fuga de información.

SI NO

7. Se cuenta con un manual de operaciones para usuario.

SI NO

8. Se cuenta con maneras de medir el desempeño del software de aplicación.

SI NO

9. Se toma en cuenta el proceso de conversión de datos para ser tomados en cuenta por otros sistemas de información.

SI NO

10. Existe documentación siempre que se implemente modificaciones a un sistema.

SI NO

11. Se cuenta con un buró de ayuda para los usuarios.

SI NO

CUESTIONARIO No. 12

PREGUNTAS DIRIGIDAS AL JEFE DE LA DIVISION DE DESARROLLO DE SISTEMAS

Objetivo:

- Verificar el desempeño de un servicio específico.

- Conocer las medidas de seguridad que se aplican a los sistemas en explotación.
- Verificar las seguridades en las cuentas de usuario.
- Verificar la seguridad de las transacciones.

1. Se cuentan con procedimientos de desempeño de un servicio específico.

   SI NO

2. Se monitorea y se reporta el desempeño de un servicio específico así como los problemas encontrados durante el procesamiento.

   SI NO

3. Las estadísticas de monitoreo son analizadas.

   SI NO

4. Se investiga las fallas y se toma acciones correctivas apropiadas.

   SI NO

5. Las medidas de seguridad se encuentren en línea con los requerimientos del negocio.

   SI NO

6. Se cuenta con un proceso de autenticación de usuarios basados en las reglas de acceso.

   SI NO

7. Existen procedimientos para conservar la efectividad de los mecanismos de autenticación y acceso.

   SI NO

8. Dicho proceso evita que personal no autorizado, conexiones telefónicas de marcado y otros puertos de entrada del sistema tengan acceso a los recursos de cómputo.

   SI NO

9. Existen procedimientos de seguridad para garantizar el control de la seguridad de acceso.

   SI NO

10. Estos procedimientos toman como base las necesidades individuales de visualización, agregación, modificación o eliminación de datos.

    SI NO

11. Existen procedimientos que aseguran acciones oportunas relacionadas con la requisición, establecimiento, emisión y suspensión de cuentas de usuario.

    SI NO

12. Existe un proceso de control establecido para revisar y confirmar periódicamente los derechos de acceso.

SI NO

13. Los usuarios controlan en forma sistemática la actividad de sus propias cuentas.

SI NO

14. Existen mecanismos que permiten supervisar la actividad normal, así como alertarlos oportunamente sobre actividades inusuales.

SI NO

15. La actividad de seguridad se registra.

SI NO

16. Se cuenta con instrumentos de control para proporcionar autenticidad a las transacciones.

SI NO

17. Se cuentan con controles cuando las transacciones no pueden ser negadas por ninguna de las dos partes (emisor y receptor).

SI NO

18. La comunicación que existe entre usuarios, entre sistemas y programas garantiza la seguridad de transacción de información.

SI NO

19. El sistema tiene seguridades para la no divulgación de claves.

SI NO

20. Poseen encriptación de claves.

SI NO

CUESTIONARIO No. 13

PREGUNTAS DIRIGIDAS AL JEFE DEL CETEIN

Objetivo:

- Conocer información del registro de la configuración.
- Conocer información de la configuración base.
- Verificar el registro de estatus.
- Verificar el control de la configuración.

1. Se registran los elementos de configuración autorizados e identificados, al momento de la adquisición.

   SI NO

2. Cuando se cambia la configuración de los equipos éstos se registran.

   SI NO

3. El registro de bitácoras y control son parte integrada del sistema de registro de configuración.

   SI NO

4. Existe una configuración base de elementos al cual regresar después de las modificaciones.

   SI NO

5. Existe seguridad en que los registros de configuración reflejan el estatus real de todos los elementos de la configuración incluyendo la historia de los cambios.

   SI NO

6. Existen procedimientos que aseguran que la existencia y consistencia del registro de la configuración sean revisadas periódicamente.

   SI NO

AUDITORIA INFORMATICA PARA DESARROLLO DE PROYECTOS

INTRODUCCIÓN

La auditoría informática para el desarrollo de proyectos abarca todas las fases que se deben seguir, desde que aparece la necesidad de disponer de un determinado sistema de información hasta que éste es construido e implantado.

Si se entiende por ingeniería del software "el establecimiento y uso de principios de ingeniería robustos, orientados a obtener software económico que sea fiable, cumpla los requisitos previamente establecidos y funcione de manera eficiente sobre máquinas reales" (Fritz Bauer)[8], la auditoría del desarrollo tratará de verificar la existencia y aplicación de procedimientos de control adecuados que permitan garantizar que el desarrollo de sistemas de información se ha llevado a cabo según estos principios de ingeniería.

OBJETIVOS

- Auditar la definición de un Plan Estratégico de Tecnología de Información.
- Auditar la definición de la Arquitectura de Información.
- Auditar la determinación de la dirección tecnológica.
- Auditar la definición de la Organización y de las Relaciones de TI.

[8] Piattini, Mario, **AUDITORIA INFORMATICA UN ENFOQUE PRACTICO**, Alfaomega Grupo Editor, S.A. de C.V., Segunda Edición, Páginas 261-262

- Auditar la comunicación de la dirección y aspiraciones de la gerencia.
- Auditar la administración de Recursos Humanos.
- Auditar la administración de proyectos.
- Auditar la administración de Calidad.
- Auditar la identificación de Soluciones.
- Auditar la adquisición y Mantenimiento de Software de Aplicación.
- Auditar el desarrollo y Mantenimiento de Procedimientos relacionados con Tecnología de Información.
- Auditar la instalación y Acreditación de Sistemas.
- Auditar la administración de Desempeño y Capacidad.
- Auditar la administración de la Configuración.

ALCANCE

Para tratar la auditoría informática del área de desarrollo es necesario, en primer lugar, acotar las funciones o tareas que son responsabilidad del área. Teniendo en cuenta que puede haber variaciones de una organización a otra, las funciones que tradicionalmente se asignan al área de desarrollo son:

- Planificación del área y participación, en la medida que corresponda, en la elaboración del plan estratégico de informática.

- Desarrollo de nuevos sistemas. Ésta es la función principal y la que da sentido al área de desarrollo. Incluirá cada uno de los sistemas, el análisis, diseño, construcción e implantación.

- Estudio de nuevos lenguajes, técnicas, metodologías, estándares, herramientas, etc. Relacionados con el desarrollo y adopción de los mismos cuando se considere oportuno para mantener un nivel de vigencia adecuado a la tecnología del momento.

- Establecimiento de un plan de formación para el personal adscrito al área.

- Establecimiento de normas y controles para todas las actividades que se realizan en el área y comprobación de su observancia.

Una vez conocidas las tareas que se realizan en el área de desarrollo, se abordará la auditoría de la misma desglosándola en dos grandes apartados:

- Auditoría de la organización y gestión del área de desarrollo.
- Auditoría de proyectos de desarrollo de sistemas de información:
    - Auditoría de la fase de análisis.
    - Auditoría de la fase de diseño.
    - Auditoría de la fase de construcción.
    - Auditoría de la fase de implantación.

MARCO TEÓRICO

Software

El software es un elemento del sistema que es lógico, en lugar de físico. Por lo tanto el software tiene unas características considerablemente distintas a las del hardware.

Aunque existen similitudes entre el desarrollo de software y la construcción del hardware, ambas actividades son fundamentalmente diferentes. En ambas actividades la buena calidad se adquiere mediante un buen diseño, pero la fase de construcción del hardware puede introducir problemas de calidad que no existen en el software.

Ambas actividades dependen de las personas, pero la relación entre las personas dedicadas y el trabajo realizado es completamente diferente para el software. Ambas actividades requieren la construcción de un producto pero los enfoques son diferentes.

El software puede aplicarse en cualquier situación en la que se haya definido previamente un conjunto específico de pasos procedimentales. El contenido y el determinismo de la información son factores importantes a considerar para determinar la naturaleza de una aplicación de software.

Algunas veces es difícil establecer categorías genéricas para las aplicaciones del software que sean significativas. Conforme aumenta la complejidad del software, es más difícil establecer

compartimientos nítidamente separados. Las siguientes áreas del software indican la amplitud de las aplicaciones potenciales:

Software de Sistemas. El software de sistemas es un conjunto de programas que han sido escritos para servir a otros programas.

Software de Tiempo Real. El software que coordina, analiza, controla sucesos del mundo real conforme ocurren, se denomina tiempo real.

Software de Gestión. Las aplicaciones en esta área reestructuran los datos existentes para facilitar las operaciones comerciales o gestionar la toma de decisiones.

Software de Ingeniería y Científico. El software de ingeniería y científico está caracterizado por los algoritmos de manejo de números.

Software Empotrado. El software empotrado reside en memoria de solo lectura y se utiliza para controlar productos y sistemas de los mercados industriales y de consumo.

Software basado en Web. Las páginas Web buscadas por un explorador son software que incorpora instrucciones ejecutables y datos.

Software de Inteligencia Artificial. El software de inteligencia artificial hace uso de algoritmos no numéricos para resolver problemas complejos para los que no son adecuados el cálculo o el análisis directo.

Planificación de Proyectos de Software.

La gestión de un proyecto de software comienza con un conjunto de actividades que globalmente se denominan planificación del proyecto. Antes de que el proyecto comience, el gestor y el equipo de software deben realizar una estimación del trabajo a realizar, de los recursos necesarios y del tiempo que transcurrirá desde el comienzo hasta el final de su realización. Siempre que estimamos, estamos mirando hacia el futuro y aceptamos resignados cierto grado de incertidumbre.

Aunque la estimación es más un arte que una ciencia, es una actividad importante que no debe llevarse a cabo de forma descuidada. Existen técnicas útiles para la estimación del esfuerzo y del tiempo. Las métricas del proyecto y del proceso proporcionan una perspectiva histórica y una potente introducción para generar estimaciones cuantitativas.

El objetivo de la planificación del proyecto de software es proporcionar un marco de trabajo que permita al gestor hacer estimaciones razonables de recursos, costo y planificación temporal. Estas estimaciones se hacen dentro de un marco de tiempo limitado al comienzo de un proyecto de software, y deberían actualizarse regularmente a medida que progresa el proyecto.

Modelos de Proceso del software.

Para resolver los problemas reales de una industria, un ingeniero del software o un equipo de ingenieros deben incorporar una estrategia de desarrollo que acompañe al proceso, métodos,

capas de herramientas y fases genéricas. Esta estrategia a menudo se llama modelo de proceso. Se selecciona un modelo de proceso para la ingeniería del software según la naturaleza del proyecto y de la aplicación, los métodos y las herramientas a utilizarse, y los controles y entregas que se requieren.

Todo el desarrollo del software se puede caracterizar como bucle de resolución de problemas en el que se encuentran cuatro etapas distintas: estado actual, definición de problemas, desarrollo técnico e integración de soluciones. El estado actual representa la situación actual de sucesos; la definición de problemas identifica el problema específico a resolverse; el desarrollo técnico resuelve el problema a través de la aplicación de alguna tecnología y la integración de soluciones ofrece los resultados.

Tipo de Modelos de Proceso de Datos.

A continuación se describen brevemente los diferentes tipos de modelo de datos:

Modelo Lineal Secuencial.

Llamado algunas veces ciclo de vida básica o modelo en cascada, el modelo lineal secuencial sugiere un enfoque sistemático, secuencial, para el desarrollo del software que comienza en un nivel de sistemas y progresa con el análisis, diseño, codificación, pruebas y mantenimiento.

Ingeniería y modelado de Sistemas. La ingeniería de información abarca los requisitos que se recogen en el nivel de empresa estratégico y en el nivel del área de negocio.

Análisis de los requisitos del software. El proceso de reunión de requisitos se intensifica y se centra especialmente en el software.

Diseño. El diseño del software es realmente un proceso de muchos pasos que se centra en cuatro atributos distintos de programa: estructura de datos, arquitectura de software, representaciones de interfaz y detalle procedimental.

Generación de código. El diseño se debe traducir en una forma legible por la máquina.

Pruebas. Una vez que se ha generado el código, comienzan las pruebas del programa.

Mantenimiento. El software indudablemente sufrirá cambios después de ser entregado al cliente.

Modelo de Construcción de Prototipos.

El modelo de construcción de prototipos comienza con la recolección de requisitos. El desarrollador y el cliente encuentran y definen los objetivos globales para el software, identifican los requisitos conocidos y las áreas del esquema en donde es obligatoria más definición. Entonces aparece un diseño rápido que se centra en una representación de esos aspectos del software que serán visibles para el usuario.

Modelo DRA (Desarrollo Rápido de Aplicaciones).

El desarrollo rápido de aplicaciones es un modelo de proceso del desarrollo del software lineal secuencial que enfatiza un ciclo de desarrollo extremadamente corto. El modelo DRA es una

adaptación a alta velocidad del modelo lineal secuencial en el que se logra el desarrollo rápido utilizando una construcción basada en componentes.

Modelado de Gestión. Se refiere al modelado del flujo de información de las funciones de gestión.

Modelado de Datos. Se definen las características de cada uno de los objetos y las relaciones entre estos objetos.

Modelado del Proceso. Los objetos de datos definidos en la fase de modelado de datos quedan transformados para lograr el flujo de información necesario para implementar una función de gestión.

Pruebas y Entrega. Como el modelo DRA enfatiza la reutilización, ya se han comprobado muchos de los componentes de los programas.

Modelo Incremental.

El modelo incremental combina elementos del modelo lineal secuencial con la filosofía interactiva de construcción de prototipos. El modelo incremental aplica secuencias lineales de forma escalonada mientras progresa el tiempo en el calendario. Cada secuencia lineal produce un incremento del software.

Modelo Espiral.

El modelo espiral es un modelo de proceso de software evolutivo que conjuga la naturaleza iterativa de construcción de prototipos con los aspectos controlados y sistemáticos del modelo lineal secuencial. En el modelo espiral, el software se desarrolla en una serie de versiones

incrementales. Durante las primeras iteraciones, la versión incremental podría ser un modelo en papel o prototipo.

Modelo de desarrollo concurrente.

El modelo de proceso concurrente se puede representar en forma de esquema como una serie de actividades técnicas importantes, tareas y estados asociados a ellas. Este modelo define una serie de acontecimientos que dispararán transiciones de estado a estado para cada una de las actividades de la ingeniería del software.

PUNTOS DE CONTROL

Los puntos de control para esta auditoria son:

- Definición de un Plan Estratégico de Tecnología de Información
- Definición de la Arquitectura de Información
- Determinación de la dirección tecnológica
- Definición de la Organización y de las Relaciones de TI
- Comunicación de la dirección y aspiraciones de la gerencia
- Administración de Recursos Humanos
- Administración de proyectos
- Administración de Calidad
- Identificación de Soluciones
- Adquisición y Mantenimiento de Software de Aplicación

- Desarrollo y Mantenimiento de Procedimientos relacionados con Tecnología de Información
- Instalación y Acreditación de Sistemas
- Administración de Desempeño y Capacidad
- Administración de la Configuración

Estos puntos de control permiten:

- Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, así como para asegurar sus logros futuros.
- Organizar de la mejor manera los sistemas de información.
- Aprovechar la tecnología disponible o tecnología emergente.
- Prestación de servicios de TI.
- Asegurar el conocimiento y comprensión del usuario sobre dichas aspiraciones.
- Maximizar las contribuciones del personal a los procesos de TI.
- Establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión.
- Satisfacer los requerimientos del cliente.
- Asegurar el mejor enfoque para cumplir con los requerimientos del usuario.
- Proporcionar funciones automatizadas que soporten efectivamente al negocio.
- Asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas.
- Verificar y confirmar que la solución sea adecuada para el propósito deseado.

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

Además se debe tomar en cuenta ciertos lineamientos para una mejor evaluación de los puntos de control:

- Definición de objetivos de negocio y necesidades de TI.
- Inventario de soluciones tecnológicas e infraestructura actual.
- Documentación.
- Diccionario de datos.
- Reglas de sintaxis de datos.
- Propiedad de la información y clasificación de severidad.
- Capacidad de adecuación y evolución de la infraestructura actual.
- Responsabilidades a nivel de alta gerencia o del consejo.
- Propiedad, custodia.
- Supervisión.
- Segregación de funciones.
- Roles y responsabilidades.
- Directrices tecnológicas.
- Compromiso con la calidad.
- Políticas de seguridad.
- Capacitación.

- La propiedad de los proyectos.
- El involucramiento de los usuarios.
- La estructuración jerárquica de tareas y los puntos de revisión.
- Asignación de responsabilidades.
- Aprobación de fases y proyecto.
- Planes y metodología de aseguramiento de calidad.
- Responsabilidades de aseguramiento de la calidad.
- Metodología del ciclo de vida de desarrollo de sistemas.
- Pruebas y documentación de sistemas y programas.
- Definición de requerimientos de información.
- Arquitectura de información.
- Pistas de auditoría.
- Contratación de terceros.
- Aceptación de instalaciones y tecnología.
- Requerimientos de usuarios.
- Requerimientos de archivo, entrada, proceso y salida.
- Interfase usuario – máquina.
- Personalización de paquetes.
- Pruebas funcionales.
- Documentación.
- Procedimientos y controles de usuarios.
- Procedimientos y controles operacionales.
- Materiales de entrenamiento.
- Capacitación.

- Carga de datos.
- Pruebas específicas.
- Acreditación.
- Herramientas de modelado.
- Administración de capacidad.
- Disponibilidad de recursos.
- Administración de cambios en la configuración.
- Controles de almacenamiento de software.

Puntos y objetivos de control.

1 Definición de un Plan Estratégico de Tecnología de Información.

1.1 Plan a largo plazo de Tecnología de Información.

1.2 Plan a largo plazo de Tecnología de Información - Enfoque y Estructura.

1.3 Cambios al Plan a largo plazo de Tecnología de Información.

1.4 Planeación a corto plazo para la función de Servicios de Información.

2 Definición de la Arquitectura de Información.

2.1 Modelo de la Arquitectura de Información.

2.2 Diccionario de Datos y Reglas de sintaxis de datos de la corporación.

2.3 Esquema de Clasificación de Datos.

2.4 Niveles de Seguridad.

3 Determinación de la dirección tecnológica.

3.1 Planeación de la Infraestructura Tecnológica.

3.2 Estándares de Tecnología.

4 Definición de la Organización y de las Relaciones de TI.

4.1 Comité de planeación o dirección de la función de servicios de información.

4.2 Funciones y Responsabilidades.

4.3 Responsabilidad del aseguramiento de calidad.

4.4 Propiedad y Custodia.

4.5 Propiedad de Datos y Sistemas.

4.6 Supervisión.

4.7 Asignación de Personal para Tecnología de Información.

4.8 Personal clave de TI.

4.9 Procedimientos para personal por contrato.

5 Comunicación de la dirección y aspiraciones de la gerencia.

5.1 Responsabilidad de la Gerencia en cuanto a Políticas.

5.2 Comunicación de las Políticas de la Organización.

5.3 Mantenimiento de Políticas.

5.4 Cumplimiento de Políticas, Procedimientos y Estándares.

5.5 Compromiso con la Calidad.

6 Administración de Recursos Humanos.

6.1 Entrenamiento de Personal.

6.2 Evaluación de Desempeño de los Empleados.

7 Administración de proyectos.

7.1 Participación del Departamento Usuario en la Iniciación de Proyectos.

7.2 Miembros y Responsabilidades del Equipo del Proyecto.

7.3 Definición del Proyecto.

7.4 Aprobación del Proyecto.

7.5 Aprobación de las Fases del Proyecto.

7.6 Plan Maestro del Proyecto.

7.7 Plan de Aseguramiento de la Calidad de Sistemas.

7.8 Plan de Prueba.

7.9 Plan de Entrenamiento.

7.10 Plan de Revisión Post Implementación de Desarrollo.

8 Administración de Calidad.

8.1 Metodología del Ciclo de Vida de Desarrollo de Sistemas.

8.2 Metodología del Ciclo de Vida de Desarrollo de Sistemas para Cambios Mayores a la Tecnología Actual.

8.3 Actualización de la Metodología del Ciclo de Vida de Desarrollo de Sistemas.

8.4 Coordinación y Comunicación.

8.5 Estándares para la Documentación de Programas.

8.6 Estándares para Pruebas de Programas.

8.7 Estándares para Pruebas de Sistemas.

8.8 Pruebas Piloto/En Paralelo.

8.9 Documentación de las Pruebas del Sistema.

8.10 Evaluación del Aseguramiento de la Calidad sobre el Cumplimiento de Estándares de Desarrollo.

8.11 Métricas de Calidad.

9 Identificación de Soluciones.

9.1 Definición de Requerimientos de Información.

9.2 Diseño de Pistas de Auditoría.

10 Adquisición y Mantenimiento de Software de Aplicación.

10.1 Métodos de Diseño.

10.2 Aprobación del Diseño.

10.3 Definición y Documentación de Requerimientos de Archivos.

10.4 Especificaciones de Programas.

10.5 Diseño para la Recopilación de Datos Fuente.

10.6 Definición y Documentación de Requerimientos de Entrada de Datos.

10.7 Definición de Interfases.

10.8 Interfases Usuario-Máquina.

10.9 Definición y Documentación de Requerimientos de Procesamiento.

10.10 Definición y Documentación de Requerimientos de Salida de Datos.

10.11 Controlabilidad.

10.12 Disponibilidad como Factor Clave de Diseño.

10.13 Materiales de Consulta y Soporte para Usuario.

10.14 Reevaluación del Diseño del Sistema.

11 Desarrollo y Mantenimiento de Procedimientos relacionados con Tecnología de Información.

- 11.1 Manual de Procedimientos para Usuario.
- 11.2 Manual de Operación.
- 11.3 Material de Entrenamiento.

12 Instalación y Acreditación de Sistemas.

- 12.1 Entrenamiento.
- 12.2 Prueba de Aceptación Final.
- 12.3 Promoción a Producción.
- 12.4 Evaluación de la Satisfacción de los Requerimientos del Usuario.
- 12.5 Revisión Gerencial Post – Implementación.

13 Administración de Desempeño y Capacidad.

- 13.1 Herramientas de Modelado.
- 13.2 Calendarización de recursos.

14 Administración de la Configuración.

- 14.1 Registro de la Configuración.
- 14.2 Base de la Configuración.
- 14.3 Registro de Estatus.
- 14.4 Control de la Configuración.
- 14.5 Almacenamiento de Software.

Estos objetivos de control se los ubica en las divisiones que se ha realizado para esta auditoría para que de esta manera sea más sencillo evaluar desde diferentes perspectivas (Organización y gestión del área de desarrollo, Proyectos de desarrollo de sistemas de información) al software en desarrollo.

Organización y gestión del área de desarrollo

- Plan a largo plazo de Tecnología de Información.
- Plan a largo plazo de Tecnología de Información - Enfoque y Estructura.
- Cambios al Plan a largo plazo de Tecnología de Información.
- Planeación a corto plazo para la función de Servicios de Información.
- Modelo de la Arquitectura de Información.
- Diccionario de Datos y Reglas de sintaxis de datos de la corporación.
- Esquema de Clasificación de Datos.
- Niveles de Seguridad.
- Planeación de la Infraestructura Tecnológica.
- Estándares de Tecnología.
- Comité de planeación o dirección de la función de servicios de información.
- Funciones y Responsabilidades.
- Responsabilidad del aseguramiento de calidad.
- Propiedad y Custodia.
- Propiedad de Datos y Sistemas.
- Supervisión.
- Asignación de Personal para Tecnología de Información.

- Personal clave de TI.
- Procedimientos para personal por contrato.
- Responsabilidad de la Gerencia en cuanto a Políticas.
- Comunicación de las Políticas de la Organización.
- Mantenimiento de Políticas.
- Cumplimiento de Políticas, Procedimientos y Estándares.
- Compromiso con la Calidad.
- Entrenamiento de Personal.
- Evaluación de Desempeño de los Empleados.
- Participación del Departamento Usuario en la Iniciación de Proyectos.
- Miembros y Responsabilidades del Equipo del Proyecto.
- Definición del Proyecto.
- Aprobación del Proyecto.
- Aprobación de las Fases del Proyecto.
- Plan Maestro del Proyecto.
- Plan de Aseguramiento de la Calidad de Sistemas.
- Plan de Prueba.
- Plan de Entrenamiento.
- Plan de Revisión Post Implementación de Desarrollo.
- Metodología del Ciclo de Vida de Desarrollo de Sistemas.
- Metodología del Ciclo de Vida de Desarrollo de Sistemas para Cambios Mayores a la Tecnología Actual.
- Actualización de la Metodología del Ciclo de Vida de Desarrollo de Sistemas.
- Coordinación y Comunicación.

- Estándares para la Documentación de Programas.
- Estándares para Pruebas de Programas.
- Estándares para Pruebas de Sistemas.
- Pruebas Piloto/En Paralelo.
- Documentación de las Pruebas del Sistema.
- Evaluación del Aseguramiento de la Calidad sobre el Cumplimiento de Estándares de Desarrollo.
- Métricas de Calidad.

Proyectos de desarrollo de sistemas de información

Fase de análisis.

- Definición de Requerimientos de Información.
- Diseño de Pistas de Auditoría.
- Herramientas de Modelado.
- Calendarización de recursos.

Fase de diseño.

- Métodos de Diseño.
- Aprobación del Diseño.
- Definición y Documentación de Requerimientos de Archivos.
- Especificaciones de Programas.

- Diseño para la Recopilación de Datos Fuente.
- Definición y Documentación de Requerimientos de Entrada de Datos.
- Definición y Documentación de Requerimientos de Procesamiento.
- Definición y Documentación de Requerimientos de Salida de Datos.
- Controlabilidad.
- Disponibilidad como Factor Clave de Diseño.
- Materiales de Consulta y Soporte para Usuario.
- Reevaluación del Diseño del Sistema.

Fase de construcción.

- Definición de Interfases.
- Manual de Procedimientos para Usuario.
- Interfases Usuario-Máquina.
- Manual de Operación.
- Material de Entrenamiento.

Fase de implantación.

- Entrenamiento.
- Prueba de Aceptación Final.
- Promoción a Producción.
- Evaluación de la Satisfacción de los Requerimientos del Usuario.
- Revisión Gerencial Post – Implementación.

- Registro de la Configuración.
- Base de la Configuración.
- Registro de Estatus.
- Control de la Configuración.
- Almacenamiento de Software.

PROCESO DE AUDITORIA

Se procede a seleccionar los puntos y objetivos de control que permitirán evaluar una área específica, finalmente se debe dirigir al capítulo No. 2 en la parte de "Examen detallado de áreas críticas".

CUESTIONARIOS DE AYUDA

CUESTIONARIO No. 1

PREGUNTAS DIRIGIDAS AL JEFE DEL CETEIN

Objetivo:

- Conocer información a cerca del modelo de la arquitectura de información.
- Conocer estándares de la sintaxis de datos.
- Conocer información del diccionario de datos.
- Conocer información de las categorías de seguridad de la información.
- Conocer información de los niveles de seguridad.

1. Es consistente la información con las necesidades planteadas.

   SI NO

2. La información obtenida permite realizar tareas eficiente y oportunamente.

SI NO

3. El modelo de arquitectura de información está acorde a las necesidades de la Armada.

   SI NO

4. El modelo de arquitectura abarca el modelo de datos corporativos y los sistemas de información asociados.

   SI NO

5. El modelo de arquitectura de información ayuda al cumplimiento del Plan Estratégico de Tecnologías de Información.

   SI NO

6. Existe un diccionario de datos corporativo.

   SI NO

7. Se cumple con los estándares de la Armada en cuanto a la definición de Tablas, Campos.

   SI NO

8. Están definidas diferentes categorías de seguridad.

   SI NO

9. Poseen responsabilidades definidas en cuanto a la información.

   SI NO

10. Existen reglas de acceso a los datos según la categoría de seguridad.

    SI NO

11. Se implementa y mantiene los niveles de seguridad para cada clasificación de datos.

    SI NO

12. A través de los niveles de seguridad se puede controlar el acceso a los datos.

    SI NO

13. Las herramientas de modelado son las apropiadas para producir un modelo del sistema actual, calibrado y ajustado según la carga de trabajo real y que sea preciso dentro de los niveles de carga recomendados.

    SI NO

14. Las herramientas de modelado se utilizan para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de la configuración, desempeño y disponibilidad.

    SI NO

15. Se lleva a cabo investigaciones técnicas profundas sobre el hardware de los sistemas.

SI NO

16. Se realizan pronósticos de futuras tecnologías.

SI NO

CUESTIONARIO No. 2

PREGUNTAS DIRIGIDAS AL JEFE DEL CETEIN

Objetivo:

- Conocer información de la planeación de la infraestructura tecnológica.
- Verificar el levantamiento de posibles cambios en un futuro.
- Conocer información de los planes de adquisición de hardware y software.
- Conocer información de estándares para el desarrollo de proyectos.

1. Se crea y actualiza regularmente planes de arquitectura de sistemas.

   SI NO

2. Se tiene un continuo monitoreo del levantamiento de requerimientos para posibles cambios en un futuro.

   SI NO

3. Existen planes de adquisición de hardware y software.

   SI NO

4. Existen estándares para el desarrollo de proyectos.

   SI NO

CUESTIONARIO No. 3

PREGUNTAS DIRIGIDAS AL JEFE DEL CETEIN

Objetivo:

- Conocer información de las funciones y responsabilidades del personal.
- Verificar si poseen procedimientos de aseguramiento de la calidad.
- Conocer información de la seguridad lógica y física.

- Conocer información de la propiedad de los datos y sistemas.
- Verificar si está identificado el personal clave.

1. El personal conoce las funciones y responsabilidades en relación con los sistemas de información.

   SI NO

2. Existen campañas regulares para aumentar la conciencia y disciplina.

   SI NO

3. Existen sistemas de aseguramiento de calidad.

   SI NO

4. Existe un grupo de aseguramiento de la calidad.

   SI NO

5. Existe un gerente de seguridad de Información.

   SI NO

6. Existe asignación de responsabilidades de seguridades adicionales.

   SI NO

7. Existe asignación de propietarios y custodios de los datos.

   SI NO

8. Existe asignación de todos los activos de información.

   SI NO

9. Existe delegación diaria de los sistemas a un administrador de seguridad.

   SI NO

10. Existe una identificación del personal clave del desarrollo de proyectos.

    SI NO

CUESTIONARIO No. 4

PREGUNTAS DIRIGIDAS AL JEFE DE LA DIVISION DE DESARROLLO DE SISTEMAS

Objetivo:

1. Verificar el cumplimiento de políticas, procedimientos y estándares.
2. Conocer información del desempeño de los empleados.
3. Conocer información de la evaluación de riesgos.

1. Existe un control interno del cumplimiento de Políticas, Procedimientos y estándares.

   SI NO

2. Existen procesos de evaluación del desempeño de empleados.

   SI NO

3. Existe una evaluación sistemática de riesgos.

   SI NO

4. Dicha evaluación contempla niveles globales y específicos del sistema.

   SI NO

5. La evaluación de riesgos contempla los activos de la organización.

   SI NO

6. La evaluación de riesgos contempla las amenazas de la organización.

   SI NO

7. La evaluación de riesgos contempla los elementos vulnerables de la organización.

   SI NO

8. La evaluación de riesgos contempla las protecciones de la organización.

   SI NO

9. La evaluación de riesgos contempla las consecuencias y probabilidades de amenaza.

   SI NO

CUESTIONARIO No. 5

PREGUNTAS DIRIGIDAS AL JEFE DEL CETEIN

Objetivo:

1. Conocer todos los pasos que se cumple para la administración de proyectos.

1. Existe un marco de referencia general para la administración de proyectos.

   SI NO

2. Interviene el departamento usuario afectado en la definición y autorización del proyecto de desarrollo.

   SI NO

3. Existe una especificación de responsabilidades y autoridades de los miembros del equipo del proyecto.

   SI NO

4. Existe un documento en el que se especifique la naturaleza y el alcance de cada proyecto.

   SI NO

5. Existe una revisión profunda de la factibilidad de los proyectos.

   SI NO

6. Existe una aprobación de cada fase antes de continuar con otra fase que forma parte del proyecto.

   SI NO

7. Existe un plan maestro que permita controlar cada fase de los proyectos.

   SI NO

8. Existen planes que aseguren la calidad de los proyectos.

   SI NO

9. Existen garantías de que los controles internos y los dispositivos de seguridad cumplan con los requerimientos necesarios.

   SI NO

10. Existe un plan de pruebas.

    SI NO

11. Existe un plan de capacitación o entrenamiento para el personal técnico.

    SI NO

12. Existe un plan de capacitación o entrenamiento para el usuario final.

    SI NO

13. Existe un plan de revisión post - implementación para cada sistema de información.

    SI NO

CUESTIONARIO No. 6

PREGUNTAS DIRIGIDAS AL JEFE DE LA DIVISION DE DESARROLLO DE SISTEMAS

Objetivo:

1. Conocer información de la metodología del ciclo de vida de desarrollo de sistemas.
2. Verificar la existencia e implementación de los estándares.

3. Verificar la existencia de un plan de pruebas.
4. Conocer si aplican métricas al software en desarrollo.

14. Existe una metodología del ciclo de vida de desarrollo de sistemas.

SI NO

15. Al requerirse cambios en el Software en Desarrollo, se asegura el cumplimiento de la Metodología del Ciclo de Vida de Desarrollo de Sistemas.

SI NO

16. Existen estándares para la documentación de programas.

SI NO

17. Existen estándares para las pruebas de los sistemas de información.

SI NO

18. Están definidas las condiciones bajo las cuales deberán llevarse a cabo las pruebas piloto o en paralelo de sistemas.

SI NO

19. Existe documentación de los resultados de las pruebas del sistema.

SI NO

20. Existen métricas para medir los resultados de las actividades.

SI NO

21. La metodología del ciclo de vida de desarrollo de sistemas asegura que los requerimientos estén claramente definidos antes de aprobar cualquier proyecto de desarrollo.

SI NO

22. Se toma en consideración el modelo de datos al definir las soluciones.

SI NO

23. Existen mecanismos adecuados para pistas de auditoria.

SI NO

24. Existe un procedimiento estándar para identificar todos los programas de software necesarios para satisfacer los requerimientos operacionales.

SI NO

25. Existe un plan de aceptación para la instalación del nuevo software.

SI NO

CUESTIONARIO No. 7

PREGUNTAS DIRIGIDAS AL JEFE DE LA DIVISION DE DESARROLLO DE SISTEMAS

Objetivo:

1. Conocer a fondo lo que comprende la metodología del ciclo de vida de desarrollo de sistemas.

1. La metodología del ciclo de vida de desarrollo de sistemas contempla métodos de diseño.

   SI NO

2. Se aplica la misma metodología del ciclo de vida de desarrollo de sistemas para todos los proyectos de desarrollo de sistemas nuevos.

   SI NO

3. La metodología del ciclo de vida de desarrollo de sistemas permite la revisión y aprobación de las especificaciones de diseño por parte del CETEIN.

   SI NO

4. La metodología del ciclo de vida de desarrollo de sistemas asegura la aplicación de un procedimiento apropiado para la definición y documentación del formato de los archivos para cada proyecto de desarrollo y modificación de sistemas de información.

   SI NO

5. La metodología del ciclo de vida de desarrollo de sistemas requiere la preparación de especificaciones detalladas por escrito de los programas para cada proyecto de desarrollo o modificación de sistemas de información.

   SI NO

6. La metodología del ciclo de vida de desarrollo de sistemas garantiza que las especificaciones de los programas correspondan a las especificaciones del diseño del sistema.

   SI NO

7. La metodología del ciclo de vida de desarrollo de sistemas requiere de la especificación de mecanismos adecuados para la recopilación y entrada de datos para cada proyecto de desarrollo y modificación de sistemas de información.

   SI NO

8. La metodología del ciclo de vida de desarrollo de sistemas requiere que existan mecanismos adecuados para definir y documentar los requerimientos de entrada de datos para cada proyecto de desarrollo o modificación de sistemas.

SI NO

9. La metodología del ciclo de vida de desarrollo de sistemas estipula que se especifiquen, diseñen y documenten apropiadamente todas las interfases internas y externas.

SI NO

10. La metodología del ciclo de vida de desarrollo de sistemas asegura el desarrollo de una interfase entre el usuario y la máquina fácil de utilizar y que sea capaz de autodocumentarse (por medio de funciones de ayuda en línea).

SI NO

11. La metodología del ciclo de vida de desarrollo de sistemas requiere la existencia de mecanismos adecuados para definir y documentar los requerimientos de procesamiento para cada proyecto de desarrollo o modificación de sistemas de información.

SI NO

12. La metodología del ciclo de vida de desarrollo de sistemas requiere la existencia de mecanismos adecuados para definir y documentar los requerimientos de salida de datos para cada proyecto de desarrollo o modificación de sistemas de información.

SI NO

13. La metodología del ciclo de vida de desarrollo de sistemas requiere que se especifiquen mecanismos adecuados para garantizar que se identifiquen los requerimientos de seguridad y control internos para proyecto de desarrollo o modificación de sistemas de información.

SI NO

14. La metodología del ciclo de vida de desarrollo de sistemas asegura que los sistemas de información estén diseñados para incluir controles de aplicación que garanticen que los datos de entrada y salida estén completos, así como su precisión, oportunidad y autorización.

SI NO

15. Se lleva a cabo una evaluación de sensibilidad durante el inicio del desarrollo o modificación del sistema.

SI NO

16. Los aspectos básicos de seguridad y control interno de un sistema a ser desarrollado o modificado son evaluados junto con el diseño conceptual del mismo.

SI NO

17. La metodología del ciclo de vida de desarrollo de sistemas asegura que la disponibilidad sea considerada en el proceso de diseño de nuevos o modificados sistemas de información en la fase más temprana posible.

SI NO

18. La disponibilidad es analizada e incrementada a través de mejoras de mantenimiento y confiabilidad.

SI NO

19. La Armada posee procedimientos para asegurar que los programas de aplicación contengan estipulaciones que verifiquen rutinariamente las tareas realizadas por el software, para apoyar el aseguramiento de la integridad de los datos y el cual haga posible la restauración de la integridad a través de procedimientos de recuperación en reversa u otros medios.

SI NO

20. La metodología del ciclo de vida de desarrollo de sistemas asegura que se preparen manuales de referencia y soporte para usuario adecuados (preferiblemente en formato electrónico) como parte de cada proyecto de desarrollo o modificación de sistemas de información.

SI NO

21. La metodología del ciclo de vida de desarrollo de sistemas asegura que el diseño de sistemas sea reevaluado siempre que ocurran discrepancias técnicas y/o lógicas durante el desarrollo o mantenimiento del sistema.

SI NO

CUESTIONARIO No. 8

PREGUNTAS DIRIGIDAS AL JEFE DE LA DIVISION DE DESARROLLO DE SISTEMAS

Objetivo:

- Conocer todo lo que tiene que ver con el software del sistema, así como el paso a producción del software.

1. Se asegura que la instalación del software del sistema no arriesgue la seguridad de los datos y programas ya almacenados en el mismo.

   SI NO

2. Existe un control para la instalación y mantenimiento de los parámetros del software del sistema.

   SI NO

3. Existen procedimientos para asegurar que el software del sistema sea instalado de acuerdo al marco de referencia de adquisición y mantenimiento de infraestructura de tecnología.

   SI NO

4. Las pruebas son realizadas antes de autorizar la utilización en ambiente de producción.

   SI NO

5. Existen procedimientos para asegurar que el software del sistema sea mantenido de acuerdo al marco de referencia de adquisición y mantenimiento para infraestructura de tecnología.

   SI NO

6. Existen procedimientos para asegurar que las modificaciones realizadas al software del sistema sean controladas de acuerdo con los procedimientos de administración de cambios de la Armada.

   SI NO

7. La metodología del ciclo de vida del desarrollo de sistemas asegura que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo de acuerdo con el plan preestablecido.

   SI NO

8. La gerencia define e implementa procedimientos formales para controlar la entrega del sistema de desarrollo a pruebas y a operación.

   SI NO

9. Los ambientes respectivos están separados y protegidos apropiadamente.

   SI NO

10. La metodología del ciclo de vida del desarrollo de sistemas requiere que una revisión post – implementación del sistema de información operacional evalúe y reporte si el sistema proporcionó los beneficios esperados de la manera más económica.

    SI NO

CUESTIONARIO No. 9

PREGUNTAS DIRIGIDAS AL JEFE DE LA DIVISION DE DESARROLLO DE SISTEMAS

Objetivo:

- Conocer que procedimientos se siguen cuando se trata de un cambio en el software.

1. Se asegura que todas las requisiciones de cambios tanto internos como por parte de proveedores estén estandarizados y sujetos a procedimientos formales de administración de cambios.

   SI NO

2. Las solicitudes se categorizan, priorizan y se establecen procedimientos para manejar asuntos urgentes.

   SI NO

3. Los solicitantes permanecen informados del estatus de la solicitud.

   SI NO

4. Existe un procedimiento para asegurar que todas las requisiciones de cambio sean evaluadas en una forma estructurada en cuanto a todos los posibles impactos sobre el sistema operacional y su funcionalidad.

   SI NO

5. Se asegura que la administración de cambios, así como el control y la distribución de software sean integradas apropiadamente en un sistema completo de administración de configuración.

   SI NO

6. Se asegura que el personal de mantenimiento tenga asignaciones específicas y que su trabajo sea monitoreado apropiadamente.

   SI NO

7. Los derechos de acceso al sistema son controlados para evitar riesgos de accesos no autorizados a los sistemas automatizados.

   SI NO

CUESTIONARIO No. 10

PREGUNTAS DIRIGIDAS AL JEFE DEL CETEIN

Objetivo:

- Conocer información a cerca de los niveles de servicio.

1. Se establece un marco de referencia en donde se presente la definición de los convenios sobre niveles formales de servicios y determine.
    - Disponibilidad.
    - Confiabilidad.
    - Desempeño.
    - Capacidad de crecimiento.
    - Niveles de soporte proporcionado al usuario.
    - Plan contingencia/recuperación.
    - Nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado.
    - Restricciones.
    - Cargos por servicio
    - Instalaciones de impresión central.
    - Distribución de impresión central.
    - Procedimientos de cambio.
2. Existe un convenio escrito que describa el nivel de servicio en términos cualitativos y cuantitativos entre los usuarios y la función de servicios de información.

    SI NO
3. El convenio define responsabilidades de ambas partes.

    SI NO
4. La función de servicios de información presta la calidad y cantidad de servicios ofrecidos.

    SI NO
5. Los usuarios ajustan los servicios solicitados a los límites acordados.

    SI NO

6. Existe un acuerdo explícito sobre los aspectos que el convenio de nivel de servicios debe tener.

   SI NO

7. El convenio de servicios cubre por lo menos los siguientes aspectos.

   - Disponibilidad,
   - Confiabilidad,
   - Desempeño,
   - Capacidad de crecimiento,
   - Niveles de soporte proporcionado a los usuarios,
   - Plan de contingencia/recuperación,
   - Nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado,
   - Restricciones,
   - Cargos por servicio,
   - Instalaciones de impresión central,
   - Distribución de impresión central,
   - Procedimientos de cambios.

8. Existen procedimientos que aseguren que la manera y responsabilidades sobre las relaciones que rigen el desempeño entre todas las partes involucradas sean establecidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.

   SI NO

9. Existe un gerente de nivel de servicio que sea responsable de monitorear y reportar los alcances de los criterios de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento.

   SI NO

10. Las estadísticas de monitoreo son analizadas regularmente.

    SI NO

11. Se investiga las fallas y se toma acciones correctivas apropiadas.

    SI NO

12. Existen procedimientos para asegurar que el contrato entre la Armada y el proveedor esté basado en niveles de procesamiento requeridos, seguridad, monitoreo, y requerimientos de contingencia.

    SI NO

13. Existe riesgo de negocios relacionado con la participación de terceros en términos de incertidumbre legal.

SI NO

CUESTIONARIO No. 11

PREGUNTAS DIRIGIDAS AL JEFE DE LA DIVISION DE DESARROLLO DE SISTEMAS

Objetivo:

1. Conocer información de la seguridad de los sistemas.

1. El acceso lógico y el uso de los recursos de Tecnología de Información están restringidos a través de la instrumentación de un mecanismo adecuado de autenticación de usuarios identificados y recursos asociados con las reglas de acceso.

SI NO

2. Dicho mecanismo evita que personal no autorizado, conexiones telefónicas de marcado y otros puertos de entrada del sistema tengan acceso a los recursos de cómputo.

SI NO

3. Dicho mecanismo minimiza la necesidad de firmas de entrada múltiple a ser utilizadas por usuarios autorizados.

SI NO

4. Existen procedimientos para conservar la efectividad de los mecanismos de autenticación y acceso.

SI NO

5. Existen procedimientos acordes con la política de seguridad que garantiza el control de la seguridad de acceso, tomando como base las necesidades individuales demostradas de visualizar, agregar, modificar o eliminar datos.

SI NO

6. Existen procedimientos que aseguran acciones oportunas relacionadas con la requisición, establecimiento, emisión y suspensión de cuentas de usuario.

SI NO

7. Existe un procedimiento de aprobación formal que indique el propietario de los datos o del sistema que otorga los privilegios de acceso.

SI NO

8. Cuenta la gerencia con un proceso de control establecido para revisar y confirmar periódicamente los derechos de acceso.

SI NO

9. Los usuarios controlan en forma sistemática la actividad de sus propias cuentas.

SI NO

10. Existen mecanismos que permiten supervisar la actividad normal, así como alertarlos oportunamente sobre actividades inusuales.

SI NO

11. Se asegura que la actividad de seguridad sea registrada y que cualquier indicación sobre una inminente violación de seguridad sea notificada inmediatamente al administrador y que las acciones consecuentes sean tomadas en forma automática.

SI NO

12. Los datos son clasificados en términos de sensitividad, mediante una decisión explícita y formal del dueño de los datos de acuerdo con el esquema de clasificación.

SI NO

13. Los datos que no requieren protección cuentan con una decisión formal que les asigne dicha clasificación.

SI NO

14. Existen controles para asegurar que la identificación y los derechos de acceso de los usuarios, así como la identidad del sistema y la propiedad de los datos, son establecidos y administrados de forma única y centralizada, para obtener consistencia y eficiencia de un control global de acceso.

SI NO

15. Existen políticas organizacionales.

SI NO

16. Las políticas organizacionales aseguran que en donde sea posible, se apliquen instrumentos de control para proporcionar autenticidad de transacciones.

SI NO

17. Aplican técnicas criptográficas para firmar y verificar transacciones.

SI NO

18. Se cuentan con controles cuando las transacciones no pueden ser negadas por ninguna de las dos partes (emisor y receptor).

SI NO

19. La comunicación que existe entre usuarios, entre sistemas y programas garantiza seguridad de transacción de información.

SI NO

20. El sistema tiene seguridades para la no divulgación de claves

SI NO

21. Poseen encriptación de claves.

SI NO

22. Existen procedimiento y protocolos para la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas.

SI NO

23. Estos procedimientos aseguran la protección de las llaves criptográficas contra modificaciones y divulgación no autorizada.

SI NO

24. Si una llave criptográfica está en riesgo, la información se hace llegar a todas las partes interesadas a través de un listado de revocación de certificados o mecanismos similares.

SI NO

25. El personal está capacitado y entrenado en los principios de seguridad de sistemas.

SI NO

26. El programa de educación y entrenamiento incluye.

- Conducta ética de la función de servicios de información.
- Prácticas de seguridad para proteger de una manera segura contra daños que afecten la disponibilidad.
- La confidencialidad, la integridad y el desempeño de las tareas.

•

CUESTIONARIO No. 12

PREGUNTAS DIRIGIDAS AL JEFE DE LA DIVISION DE DESARROLLO DE SISTEMAS

Objetivo:

1. Conocer información referente a la configuración del software.

1. Son registrados únicamente elementos de configuración autorizados e identificados en el inventario, al momento de la adquisición.

   SI NO

2. Existen procedimientos para dar seguimiento a los cambios en la configuración.

   SI NO

3. El registro de bitácoras y control son parte integrada del sistema de registro de configuración.

   SI NO

4. Existe una configuración base de elementos como punto de verificación al cual regresar después de las modificaciones.

   SI NO

5. Existe seguridad en que los registros de configuración reflejan el estatus real de todos los elementos de la configuración incluyendo la historia de los cambios.

   SI NO

6. Existen procedimientos que aseguran que la existencia y consistencia del registro de la configuración sean revisadas periódicamente.

   SI NO

CUESTIONARIO No. 13

PREGUNTAS DIRIGIDAS AL JEFE DE LA DIVISION DE DESARROLLO DE SISTEMAS

Objetivo:

- Conocer los procedimientos de todo lo que tiene que ver con los datos.

1. Existen procedimientos de preparación de datos a ser seguidos por los departamentos usuarios.

SI NO

2. El diseño de formas de entrada de datos ayuda a minimizar errores y omisiones.

SI NO

3. Existen procedimientos para manejo de errores.

SI NO

4. Dichos procedimientos aseguran razonablemente que los errores y las irregularidades sean detectados, reportados y corregidos.

SI NO

5. Existe seguridad que los documentos fuente son preparados apropiadamente por personal autorizado.

SI NO

6. Se establece una separación de funciones adecuadas con respecto al origen y aprobación de documentos fuente.

SI NO

7. Existen procedimientos que aseguran que todos los documentos fuente autorizados estén completos, sean precisos, registrados apropiadamente y transmitidos oportunamente para la entrada de datos.

SI NO

8. Existen procedimientos de manejo de errores durante la creación de datos de entrada.

SI NO

9. Estos procedimientos aseguran razonablemente que los errores y las irregularidades sean detectados, reportados y corregidos.

SI NO

10. Existen procedimientos que aseguran que la organización pueda retener o reproducir los documentos fuentes originales durante un período de tiempo razonable.

SI NO

11. Dichos procedimientos facilitan la recuperación o reconstrucción de datos

SI NO

12. Dichos procedimientos satisfacen requerimientos legales.

SI NO

13. Existen procedimientos apropiados para asegurar que la entrada de datos sea llevada a cabo únicamente por personal autorizado.

SI NO

14. Los datos sobre transacciones, capturados para su procesamiento están sujetos a una variedad de controles para verificar su exactitud, suficiencia y validez.

    SI NO

15. Existen procedimientos que aseguran que los datos de entrada sean validados y editados tan cerca del punto de origen como sea posible.

    SI NO

16. Existen procedimientos para la corrección y reenvío de datos que hayan sido capturados erróneamente.

    SI NO

17. Existen procedimientos para el procesamiento de datos que aseguren que la segregación de funciones sea mantenida.

    SI NO

18. Existen procedimientos para el procesamiento de datos que aseguren que el trabajo realizado sea verificado rutinariamente.

    SI NO

19. Dichos procedimientos aseguran que se establezcan controles de actualización adecuados como totales de control y controles de actualización de archivos maestros.

    SI NO

20. Existen procedimientos para asegurar que la validación, autenticación y edición del procesamiento sean llevadas a cabo tan cerca del punto de origen como sea posible.

    SI NO

21. Existen procedimientos de manejo de errores en el procesamiento de datos que permitan la identificación de transacciones erróneas sin que éstas sean procesadas y sin interrumpir el procesamiento de otras transacciones válidas.

    SI NO

22. Existen procedimientos para el manejo y retención de datos de salida de sus programas de aplicación de tecnología de información.

    SI NO

23. Existen procedimientos escritos para la distribución de datos de salida de tecnología de información.

    SI NO

24. Existen procedimientos para asegurar que los datos de salida sean balanceados rutinariamente con los totales de control relevantes.

SI NO

25. Existen pistas de auditoría para facilitar el seguimiento del procesamiento de transacciones y la conciliación de los datos con problema.

SI NO

26. Existen procedimientos para asegurar que la precisión de los reportes de los datos de salida sea revisada por el proveedor y usuarios relevantes.

SI NO

27. Existen procedimientos para controlar los errores contenidos en los datos de salida.

SI NO

28. Existen procedimientos para garantizar que la seguridad de los reportes de datos de salida sea mantenida para todos aquellos reportes que estén por distribuirse.

SI NO

29. Se asegura que durante la transmisión y transporte de información sensible, se proporcione una adecuada protección contra acceso o modificación no autorizada, así como contra envíos a direcciones erróneas.

SI NO

30. Existen procedimientos para impedir la divulgación indebida o el desecho de información delicada de la organización.

SI NO

31. Dichos procedimientos garantizan que ninguna información marcada como borrada o desechada, pueda ser accedida por personas internas o externas a la organización.

SI NO

32. Existen procedimientos para el almacenamiento de datos que consideren requerimientos de recuperación, de economía y las políticas de seguridad.

SI NO

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Las auditorías informáticas se materializan recopilando información y documentación de todo tipo. Los Informes finales de los auditores dependen de su destreza para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. Por lo tanto se concluye que:

- El Campo de la Auditoría Informática se basa en:
  1. La evaluación administrativa del área de informática.
  2. La evaluación de los sistemas y procedimientos, y de la eficiencia que se tiene en el uso de la información. La evaluación de la eficiencia y eficacia con la que se trabaja.
  3. La evaluación del proceso de datos, de los sistemas y de los equipos de cómputo (software, hardware, redes, bases de datos, comunicaciones).
  4. Seguridad y confidencialidad de la información.
  5. Aspectos legales de los sistemas y de la información.

- Los principales objetivos de la auditoría informática son los siguientes:
  1. Salvaguardar los activos (hardware, software y recursos humanos).
  2. Integridad de datos.
  3. Efectividad de sistemas
  4. Eficiencia de sistemas.
  5. Seguridad y confidencialidad.

- El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, también llamados evidencias.

- Los procedimientos de auditoría informática varían de acuerdo con la filosofía y técnica de cada organización y departamento de auditoría en particular.

- La proliferación de la tecnología de información ha incrementado la demanda de control de los sistemas de información, como el control sobre la privacidad de la información y su integridad, y sobre los cambios de los sistemas, entre otros.

- Todos los programas o paquetes empleados en la auditoría deben permanecer bajo estricto control del departamento de auditoría. Por esto, toda la documentación, material de pruebas, listados fuente, programas fuente y objeto, además de los cambios que se les hagan, serán responsabilidad del auditor.

Recomendaciones

Este manual es una referencia de cómo se debería realizar una Auditoría Informática, dependiendo del área a ser auditada, pero este manual no delimita el alcance de cada tema que compone el ambiente informático, el alcance dependerá de hasta donde quiere llegar el Auditor o el equipo de Auditoría. Por lo que se recomienda:

- El éxito de realizar una Auditoría Informática no radica simplemente en la aplicación de los temas desarrollados en este manual, sino dependerá del grado de compromiso de la Armada para aceptar un informe de auditoría.

- Se recomienda la participación de personal especializado en las diferentes áreas planteadas en este manual, con esto se asegura que cada área será analizada de manera minuciosa.

- Se recomienda la revisión y actualización de este manual por lo menos una vez al año ó de acuerdo al grado evolutivo que tenga la Armada en tecnología.

- Se recomienda que los planes de auditoria informática se realicen anualmente y que cuente con la asignación de recursos humanos, económicos y técnicos.

- Se recomienda revisar los puntos de control de COBIT, ya que este manual se fundamenta en los puntos de control que ahí se exponen.