ULACIT
Universidad Latinoamericana de Ciencia y Tecnología

LICENCIATURA EN INGENIERÍA INFORMÁTICA

TEMA

ASPECTOS QUE SE DEBEN CONSIDERAR PARA LA IMPLEMENTACIÓN DE UN CENTRO DE GESTIÓN EN EL CENTRO DE TECNOLOGÍA DE INFORMACIÓN DE LA JUNTA DE PENSIONES Y JUBILACIONES DEL MAGISTERIO NACIONAL EN LO QUE CONCIERNE A SEGURIDAD, SOPORTE Y CONTINGENCIA UTILIZANDO LA NORMA ISO 9004 "SISTEMAS DE GESTIÓN DE LA CALIDAD – DIRECTRICES PARA LA MEJORA DEL DESEMPEÑO"

Sustentante: Ángela Tencio Chacón

PROYECTO DE GRADUACIÓN PARA OPTAR POR EL GRADO DE LICENCIATURA EN INGENIERÍA INFORMATICA.

San José - Costa Rica
Junio, 2004

DECLARACIÓN JURADA

Yo Ángela Tencio Chacón alumna de la Universidad Latinoamericana de Ciencia y Tecnología (ULACIT), declaro bajo la fe de juramento y consciente de la responsabilidad penal de este acto, que soy e autor intelectual de la Tesis de Grado titulada: Aspectos que se deben considerar para la implementación de un Centro de Gestión en el Centro de Tecnología de Información de la Junta de Pensiones y Jubilaciones del Magisterio Nacional en lo que concierne a seguridad, soporte y contingencia utilizando la Norma ISO 9004 "Sistemas de Gestión de la Calidad –Directrices para la mejora del Desempeño", por lo que libero a la ULACIT, de cualquier responsabilidad en caso de que mi declaración sea falsa.

Brindada en San José – Costa Rica en el día 25 del mes de junio del año dos mil cuatro.

_____

Cédula de Identidad: 1-979-570

ULACIT

Universidad Latinoamericana de Ciencia y Tecnología

TRIBUNAL EXAMINADOR

Reunido para los efectos respectivos, el Tribunal Examinador de la Escuela de Posgrados compuesto por:

Lic. Rodney Herrera López

Tutor

MSc. Wilberth Molina Perez

Director del CIDE

Master Mauricio Vega Díaz

Presidente del Tribunal

AGRADECIMIENTO

A Dios por darme el don la vida, sabiduría
e iluminar mi camino.

Al Lic. Rodney Herrera por su constante guía y
consejo para la finalización del presente
trabajo de investigación.

A mis padres, hermanos y amigos
que de una u otra forma brindaron su apoyo y
colaboración para culminar mi meta.

INDICE DE CONTENIDOS

CAPÍTULO I

INTRODUCCIÓN

Las medidas de seguridad son un aspecto básico en el proceso de información, su pilar fundamental se enfoca en el mantenimiento mínimo de riesgo, donde se pueden ver afectados el recurso humano, los servicios, los equipos y la información; esto debido a que existe gran variedad de sucesos, de diversa naturaleza que pueden dificultar o impedir el modo normal de operación de un Centro de Tecnología de Información.

Freedman define seguridad como la "Protección de datos contra el acceso no autorizado. Los programas y datos se pueden asegurar entregando números de identificación y contraseñas a los usuarios autorizados de una computadora. Sin embargo los programadores de sistemas, u otros individuos técnicamente competentes, pueden llegar a acceder a estos códigos". (1993, pág 697). La seguridad abarca todas aquellas disposiciones que tienen como fin eliminar las acciones y riesgos que en un momento dado se pueden presentar y afectar la información y los recursos existentes en el Centro de Tecnología de Información (CTI) de la Junta de Pensiones y Jubilaciones del Magisterio Nacional, así como los planes de contingencia en caso de desastre.

El desarrollo del informe está dividido en seis capítulos, estructurados de la manera siguiente:

En el primer capítulo se indican los aspectos informativos de la investigación, el análisis situacional, se formula el problema, los objetivos, así como las variables que serán tratadas en el estudio.

En el segundo se consideran los aspectos teóricos que sirven de base para sustentar mediante una mayor comprensión conceptual las variables y su relación.
En el capítulo tercero se plantea la metodología utilizada en la realización del trabajo, incluyendo el tipo de investigación, las fuentes de información, y se describen los instrumentos utilizados para recolectar los datos.

En el cuarto se obtienen los resultados producto de la investigación, se representan los datos de manera tabulada y organizados secuencial y sistemáticamente.

En el quinto capítulo se incluyen las conclusiones y recomendaciones en relación con las variables investigadas, lo que permite cumplir con la solución al problema planteado en la investigación.

En el sexto capítulo se realiza la propuesta para la implementación de un Centro de Gestión en el Centro de Tecnología de Información de la Junta de Pensiones y Jubilaciones del Magisterio Nacional, con el fin de mantener un control de calidad preventivo y correctivo en lo que corresponde a seguridad, soporte y contingencia.

EL PROBLEMA Y SU IMPORTANCIA

1. Aspectos Situacionales

1.1 Junta de Pensiones y Jubilaciones del Magisterio Nacional

La siguiente reseña fue recopilada del libro Ley del Sistema de Pensiones y Jubilaciones del Magisterio Nacional. El marco legal histórico que da soporte a la existencia de la Junta se inicia con diversas instituciones que anteceden lo que es hoy en día la Junta de Pensiones. Se inicia con la Ley de Pensiones para Maestros Titulados en 1866. Posteriormente, en 1920 se dedica en el Código de Instrucción Pública un capítulo sobre las pensiones y jubilaciones de los educadores. En 1923 se decreta una Ley que rige hasta 1958, en que por mandato de la Ley 2248, se crea la junta de Pensiones y Jubilaciones del Magisterio Nacional como la administradora técnica y financiera de Fondo, disposición que se dio hasta el 19 de noviembre de 1991; con la aprobación de la Ley 7268. A partir de ella se modifica la Ley 2248. De esta manera se crea el Fondo de Capitalización de Pensiones del Magisterio Nacional en julio de 1992, según Ley 7302 artículo 39, en la que la junta será la administradora jurídica y financiera con toda soberanía.

1.2 Los beneficios para los trabajadores del Magisterio

Los trabajadores que gozan beneficios de los servicios que la junta ofrece son todos aquellos docentes y administrativos de los centros de enseñanza pública y privada de educación preescolar, primaria y secundaria, además los trabajadores de centros universitarios.

1.3 Misión de la Junta de Pensiones

Según indica el libro "Ley del Sistema de Pensiones y Jubilaciones del Magisterio Nacional" la misión de la empresa es "Administrar técnica y jurídicamente dentro del marco de los principios de Seguridad Social, el Sistema de Pensiones y Jubilaciones de Magisterio Nacional, para satisfacer el retiro y mejorar la calidad y el nivel de vida de nuestra membresía."(Contraportada, 2000)

1.4 Visión de la Junta de Pensiones

El libro "Ley del Sistema de Pensiones y Jubilaciones del Magisterio Nacional" cita como visión "Somos una Institución sólida modelo de gestión y servicio, que garantiza el retiro y mejoramiento de la calidad y el nivel de vida de nuestra membresía."(Contraportada, 2000)

1.5 Desarrollo Tecnológico de la Junta de Pensiones

Durante sus primeros 35 años la Institución no se esforzó en brindar servicio de calidad a sus clientes; aun más, ni siquiera los consideraba como tales por cuanto la pertenencia al Régimen era de carácter obligatorio y la demanda de servicio consistía en el trámite de pensiones y derivados, así como la información resultante del estudio de pensiones o jubilaciones.

Se mantuvo efectuando procesos manuales, sin automatizarlos, por lo que no se contaba con información veraz y oportuna y la capacidad de respuesta a las demandas de servicio era tardía. En un principio esta demanda de servicios no era significativa en términos de cuantas personas lo solicitaban ni de la información necesaria para resolver; pues un Régimen de Pensiones tarda cerca de 35 ó 40 años en madurar, luego de su nacimiento.

De allí que en 1990 se empiece a sentir el impacto del creciente número de personas con derecho a pensión y el engrosamiento de las filas de pensionados y jubilados y con ello, la urgencia de contar con información veraz y oportuna. Entonces se procede a subcontratar servicios informáticos a la Caja de Ande, otra institución de economía solidaria del Magisterio, que había adquirido un moderno equipo de cómputo IBM y le ofreció a la Junta trabajarle aprovechando la excesiva capacidad del mismo. En realidad, consistía en la digitación de la información así como convertirla a cintas magnéticas que eran entregadas en la Dirección General de Informática del Ministerio de Hacienda para proceder al pago de pensiones del Régimen. Además corría algunos procesos como el cálculo de costos de vida para pensionados. Los pagos que por estos conceptos hacía la Junta a la Caja de Ande eran millonarios y exorbitantes.

En 1992 se nombra un nuevo Director Ejecutivo, hombre visionario que reconoce esta debilidad de la institución e inicia un proceso de automatización y desarrollo informático de la administración de la información, la cual " tiene la capacidad de revitalizar el negocio y crear ventajas competitivas, siempre y cuando después de analizarla y procesarla se tomen acciones y se hagan cambios con base en esa información".(Luigi Valdés, Conocimiento es Futuro, p.32).

Se procede a contratar un asesor informático de reconocida trayectoria en el ámbito académico y empresarial y, en equipo diseñar el futuro informático de la Institución pasando de una era de "oscurantismo" a la era de la automatización de procesos así como recopilación y procesamiento de datos. A criterio del asesor, "el proceso de modernización de la Junta resulta muy interesante, pues en el 90 era una Institución sin ningún apoyo informático y en memos de un año se puso a la vanguardia entre las instituciones del Magisterio, con una fuerte inversión en software y hardware".

En el proceso de automatización se valoran situaciones como la necesidad de administrar su propia información, correr sus propios procesos, contar con la información que los clientes requieren, llevar un estricto control de los crecientes trámites, entre otros. El asesor advierte la necesidad de que las herramientas que se adquirieran, tanto el hardware como el software, deberían atender no sólo la demanda actual sino la futura. Se recomienda arquitectura RISC, lenguaje de cuarta generación y una fuerte infraestructura de red. Luego de un extenso análisis se presenta a la Junta Directiva el proyecto y se inicia el proceso de licitación. Entre las empresas que participan se encuentran Datatec, IBM, Control Electrónico, Unisys CESA y Oracle. Se escoge CESA para la compra del hardware, mientras que el motor de base de datos se compra directamente de la empresa ORACLE, que ofrece además la capacitación para el personal responsable. Esta elección se efectuó con base en los requerimientos técnicos y la relación costo-beneficio.

De igual manera se inicia una "campaña de concientización de la urgencia de servicio" que debía alcanzar a toda la organización pues la excelencia en el servicio a los clientes externos comienza proveyendo un servicio sobresaliente a los compañeros de trabajo.

A partir de las herramientas adquiridas, la Institución procedió a contratar y capacitar profesionales en informática para el desarrollo interno y mantenimiento de los sistemas y procesos que resultaran necesarios para la correcta gestión en todas sus áreas.

El desarrollo de los sistemas se ha efectuado de manera interna por lo que se creó el CTI que cuenta actualmente con la jefatura, secretaria, seis analistas de

sistemas y programadores a la vez, uno de los cuales es el administrador de la base de datos (DBA) y dos funcionarios de soporte técnico.

Desde 1992 la Junta se ha esmerado por brindar sus servicios de la mejor manera, en virtud de lo cual se ha esforzado por abastecerse de la infraestructura adecuada, los medios informáticos de avanzada y el personal idóneo para lograr un lugar de privilegio entre las organizaciones magisteriales.

2. Antecedentes

El desarrollo tecnológico en el campo de los sistemas utilizados en las organizaciones ha llegado a tal nivel en los últimos años que con dificultad se encuentra actualmente una institución u organización, cualquiera que ésta sea, que no cuente ya con equipos de cómputo como herramientas para su proceso diario de información. En su inicio, el equipo de cómputo y los sistemas de información basados en computadora soportaban sólo el control de funciones operacionales básicas, tales como inventarios, nómina, administración y contabilidad; sin embargo, su uso se ha extendido en la actualidad al desarrollo de sistemas basados en el conocimiento utilizados por la administración de la organización en la toma de decisiones. Es por ello que la creciente concentración de la información en sistemas computacionales y, por consiguiente, la elevada dependencia a los sistemas, las hacen vulnerables a las organizaciones respecto a la pérdida, daño o uso indebido de la información.

Parte de la seguridad del CTI es cubrir las amenazas ocasionadas tanto por el ser humano como por la naturaleza del medio físico donde se encuentra ubicado el CTI; algunas de estas amenazas son: desastres naturales, incendios accidentales, inundaciones; entre las hechas por el hombre se pueden mencionar: disturbios, sabotajes internos y externos deliberados.

Actualmente las empresas deben estar preparadas para tratar de evitar al máximo la ocurrencia o minimizar las pérdidas causadas por un desastre informático. El hecho de contar con medidas de seguridad de la información es el factor esencial para que una empresa logre minimizar el impacto producido por un percance de este tipo; además, Echenique indica que "la información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos"(1990, pág 102).

Además, es importante contar con Planes de Contingencia con el objetivo de mantener el servicio a los usuarios críticos a pesar de la calamidad dado que todas las empresas son vulnerables. Luis Angel Rodríguez indica que un Plan de Contingencia "es un plan escrito en el que se detallan acciones, procedimientos y recursos que deben usarse durante un desastre que cause destrucción parcial o total de los servicios de computación". (1995,pág 161)

3. Delimitación del problema

Las consecuencias a las que se exponen las organizaciones, en caso de llegar a perder los recursos informáticos o tener que realizar sus operaciones sin ellos, hace que se valore la seguridad del Centro de Tecnología de Información de la Junta de Pensiones y Jubilaciones del Magisterio Nacional como un aspecto de suma importancia; ya que parte de estos recursos son su centro de actividad y se utilizan para su funcionamiento todos los días ("hardware", "software", datos y personas).

AUDISIS indica "Es recomendable que todas las organizaciones establezcan un plan de seguridad en sus Centros de Procesamiento con el objetivo de proporcionar medidas de seguridad razonables y suficientes para permitirles que

ejecuten las funciones establecidas sin interrupciones y sin perder y/o divulgar la información de la empresa". (1994, pág 3)

Jaime Arellano define problema como: "Fijar los límites a los que va a llegar el tema, es establecer claramente lo que se va a tratar o investigar, al realizar la formulación del problema se debe delimitar o definir". (1990, pág 78)

Con base en la información mencionada anteriormente se plantea el problema de la investigación:

¿Qué aspectos se deben considerar para la implementación de un Centro de Gestión en el Centro de Tecnología de Información de la Junta de Pensiones y Jubilaciones del Magisterio Nacional en lo que concierne a seguridad, soporte y contingencia utilizando la norma ISO 9004 "Sistemas de Gestión de la Calidad – Directrices para la mejora del Desempeño"?

4. Justificación

La seguridad en los Centros de Tecnología de Información es una necesidad, por lo que se deben establecer reglas y medidas que permitan garantizar el perfecto funcionamiento de los equipos de cómputo, su disponibilidad permanente y para lograrlo se necesita disminuir o eliminar cualquier situación que represente una amenaza a la continuidad en las operaciones. La seguridad y protección de la información juega un papel de suma importancia, pues encierra los "datos" que es el activo más valioso y estratégico en una organización para la toma de decisiones, de forma oportuna y confiable; por lo que se encuentra expuesto a robos, fraudes o sabotajes que podrían causar una destrucción total o parcial de la actividad organizacional. Además se debe considerar que la seguridad no es

algo tangible, ni produce dividendos, pero cuando no se tiene pueden darse situaciones catastróficas.

Para protegerlas de esta vulnerabilidad se requiere conocer las funciones, políticas, procedimientos y métodos por seguir para garantizar una seguridad razonable de la información que se maneja y de esta forma minimizar los impactos de un riesgo, si éste se llegara a concretar.

PROPÓSITO DEL ESTUDIO

1. Objetivos

1.1 Objetivo General de Diagnóstico

Analizar el nivel de seguridad, soporte y lo concerniente a planes de contingencia del Centro de Tecnología de Información, para garantizar la protección de la información, el adecuado funcionamiento y la continuidad de las operaciones.

1.2 Objetivo General de Solución

Proponer un modelo de Centro de Gestión para controlar la seguridad del CTI, en cuanto a hardware y software, soporte y contingencia y de esta forma contar con una estandarización de los procesos, una mejora continua y salvaguarda de los recursos.

1.3 Objetivos Específicos

- Identificar los procedimientos existentes en lo concerniente a seguridad y soporte en el Centro de Tecnología de Información.

- Determinar los recursos de hardware y software por ser evaluados dentro del Centro de Tecnología de Información.

- Identificar los factores por los que se puede ver afectada la seguridad física del Centro de Tecnología de Información.

- Identificar los factores que se toman en cuenta para la protección de la información.

- Identificar las políticas establecidas actualmente para una eventual contingencia.

- Identificar la factibilidad económica requerida que garantice la implementación del Centro de Gestión.

2. Definición de Variables

Variable N°1: Procedimientos existentes

Definición Conceptual

Los procedimientos constituyen la manera de hacer las cosas en forma ordenada y sistemática para cumplir un determinado objetivo.

Definición Operacional

Se identifica si el Centro de Tecnología de Información cuenta con procedimientos para llevar a cabo operaciones de seguridad tanto física como lógica y de soporte.

Variable N°2: Hardware y Software

Definición Conceptual

Hardware es la parte que la persona puede observar y tocar del equipo de cómputo, o bien la parte física y el equipo asociado. Se encuentra formado entre

otros por el procesador el cual se encargan de manipular los datos, interpretar y ejecutar instrucciones; unidades de memoria que se encarga de dar al procesador almacenamiento temporal para programas y datos lo que permite que se guarden y recuperen de forma rápida; dispositivos de entrada / salida que son la manera en que la máquina se comunica con los usuarios y con otras máquinas o dispositivos, entre éstos se encuentran el teclado, mouse, pantallas, lectores, impresoras, entradas de voz, entre otros; y dispositivos de almacenamiento que son los que permiten almacenar los datos en forma permanente; estos pueden ser en forma magnética (discos flexibles, discos duros, cinta magnética) y el almacenamiento óptico (CD-ROM, WORM, medios magnético-ópticos).

En lo que corresponde a Software, es el conjunto de instrucciones ordenadas en forma lógica que cuando son ejecutadas le indican a la computadora que realice ciertas tareas lo que permite la manipulación de los datos; el software no serviría de nada, sino está ligado al "hardware" pues son un complemento; su desarrollo crece de acuerdo con plataforma de hardware y las exigencias de los usuarios; se clasifican en tres categorías: sistemas operativos, lenguajes de programación y software de aplicación.

Definición Operacional

Se identifican las características del equipo y el software con que cuenta el Centro de Tecnología de Información para ser considerados dentro del modelo por proponer.

Variable N°3: Factores de la seguridad física

Definición Conceptual

La seguridad física trata de proteger los Centros de Tecnología de Información. Tiene como objetivo establecer políticas, procedimientos y prácticas para evitar

las interrupciones prolongadas del servicio de procesamiento de datos y disminuir o evitar la exposición a riesgo, ya sean internos o externos al Centro de Tecnología de Información o sean procedentes de la naturaleza o del hombre.

Definición Operacional

Se identifican los riesgos ya sean internos o externos procedentes de la naturaleza o del hombre que pueden afectar al Centro de Tecnología de Información tales como incendios, inundaciones, terremotos, disturbios, cortes de fluido eléctrico, acceso al centro de tecnología, entre otros.

Variable N°4: Factores para la protección de la información

Definición Conceptual

La protección de la información incluye normas para el control del acceso a los datos / información, a fin de reducir el riesgo de transferencia, modificación, pérdida o divulgación accidental o intencional de ésta, además de garantizar que las operaciones sean realizadas únicamente por las personas autorizadas.

Definición Operacional

Se identifican los procedimientos utilizados por el Centro de Tecnología de Información para controlar el acceso a la información y de ésta forma evitar la pérdida y la incorrecta manipulación de los datos.

Variable N°5: Políticas actuales para enfrentar Contingencia

Definición Conceptual

El plan de contingencia es una herramienta de prevención e instrucción a posibles eventualidades que puedan ocurrir, como tal, esta herramienta se fundamenta en estudios de importancia de las diferentes actividades que se realizan en un área

de trabajo y de acuerdo con las necesidades de la empresa, como son los mecanismos mínimos con los cuales se debe contar para solventar una emergencia y así permitir a la institución ofrecer los servicios informáticos principales de forma transparente para los usuarios.

Definición Operacional

Se identifican las políticas establecidas por el Centro de Tecnología de Información utilizadas en caso de una eventualidad, que llegue a desestabilizar el proceso normal de operación.

Variable N°6: Factibilidad Económica

Definición Conceptual

La factibilidad económica mide la efectividad y costo de un proyecto, es lo que se denomina costo/beneficio. El análisis del costo involucra la erogación de dinero o recursos que se requerirán para el desarrollo del proyecto y su operación; los beneficios generalmente aumentan las ganancias y disminuyen los costos, pueden ser tangibles, cuantificables (tiempo, utilización de recursos) o intangibles, no se pueden cuantificar (satisfacción del cliente)

Definición Operacional

La factibilidad económica involucra el análisis del costo del proyecto considerando el valor de los recursos necesarios para la implementación contra los beneficios obtenidos en cuanto a la seguridad.

Variable N°7: Modelo de Centro de Gestión

Definición Conceptual

El modelo tiene como objetivo asegurar la estandarización de los procesos operativos, promover la coordinación de actividades y la ejecución de una gestión eficiente y mejora continua que garantice un mejor servicio al cliente interno y externo.

Definición Operacional

El Centro de Gestión constituye una comisión o área la cual va a apoyar la actualización y mejoramiento de los procesos de seguridad, soporte y contingencia que se realizan en el CTI y en conjunto con el Comité de Informática apoyar el desarrollo informático institucional.

CAPÍTULO II: MARCO TEÓRICO

La tecnología informática ha revolucionado los negocios en todo el mundo, pues prácticamente todas las organizaciones, grandes o pequeñas, dependen de equipos de procesamiento de información para automatizar o ayudar en sus actividades diarias y así lograr ser eficientes en la producción de bienes y servicios de alta calidad. Sin las computadoras, que ayudan al proceso y suministro de información precisa y actualizada que se necesita para la toma de decisiones estratégicas y administrar los procesos de producción, muchas empresas no podrían subsistir.

La Junta de Pensiones no ha sido la excepción y con el fin de mantenerse dentro de un mundo dinámico y cambiante en lo que se refiere a tecnología, utiliza la informática como una herramienta en su quehacer diario, la cual permite tener la mayor cantidad de datos en forma precisa y de fácil acceso.

El CTI de la Junta de Pensiones se encuentra conformado por equipo de cómputo (hardware), software (que indica a la computadora qué hacer) y el personal que ejecuta los programas, desarrolla el software y brinda soporte técnico, el cual debe ser capaz de manejar las necesidades de información de la institución, de forma que pueda almacenar, transmitir, procesar y recuperar en forma electrónica los datos y por ende la información; además, controla el funcionamiento normal y diario del hardware y software del Sistema de Información.

Es importante señalar que las personas son las responsables de las operaciones dentro del CTI e interactúan, con el fin de apoyar las actividades de la institución junto con los Sistemas de Información.

Por lo tanto, es primordial saber con qué equipo cuenta el CTI, además de sus especificaciones ya sea de software o hardware.

La institución depende en parte, de la información que se procesa, para realizar las funciones y para la toma de decisiones, por lo que es vulnerable a la pérdida, daño o uso indebido de la información.

Es entonces necesario que la Junta de Pensiones tome conciencia de la importancia que tiene proteger sus recursos informáticos y las graves consecuencias que puede traer la pérdida o inhabilitación de su funcionamiento. Así como la responsabilidad que tiene al manejar información confidencial de los usuarios, por lo que resulta indispensable tener un programa integral de información y prepararse contra una eventual contingencia.

Por lo tanto, la institución debe contar con un ambiente de seguridad razonable para lograr una actividad adecuada, que le permita tener la confianza de que sus activos como lo son el hardware, el software y el recurso humano, están debidamente protegidos.

De aquí la importancia de revisar y controlar que la información se administre en forma apropiada, y que se encuentre protegida y asegurada contra riesgos como lo son: accesos no autorizados, pérdida de datos e información, desfalcos, robo, desastres naturales y actividades erróneas.

Dado lo anterior, la seguridad de la información juega un papel importante ya que el hecho de que los desastres no se produzcan todos los días, sino en forma ocasional, no significa que la situación esté totalmente controlada. Todos los días pueden ocurrir robos de información, incendios y aún sabotajes contra las instalaciones del CTI, además desastres naturales, tales como terremotos, inundaciones, entre otras, que van afectar la información de una u otra manera.

Con el fin de minimizar estos riesgos, se deben establecer características apropiadas de seguridad y controles por medio de políticas y procedimientos que permitan asegurar la salvaguarda de los recursos.

Como parte de la seguridad física se debe considerar que exista una protección adecuada y una salvaguarda de la instalación física del computador; se deben establecer un conjunto de procedimientos para disminuir o evitar la exposición a riesgo, ya sean internos o externos al CTI; como pueden ser los incendios, inundaciones, terremotos, disturbios, cortes de fluido eléctrico, entre otros.

En lo que corresponde a la seguridad lógica se debe asegurar que el contenido de los archivos de información no estén expuestos a alteraciones no autorizadas y que contienen la información completa, correcta autorizada y consistente, además de que exista una bitácora en caso de ser necesario para mostrar cuándo y quién creó o modificó un archivo en particular.

De aquí la importancia de desarrollar en forma amplia los elementos que se ven involucrados en cada una de las áreas, tanto la seguridad física como la lógica.

Contar por escrito con un detalle de las acciones, procedimientos y recursos que deben ser utilizados en caso de desastre que cause destrucción parcial o total de los servicios de computación, es fundamental para garantizar el funcionamiento mínimo del CTI. Deben de estar definidas las tareas críticas, quién es el responsable de todos los aspectos del proceso de recuperación y la forma de trabajo mientras se vuelve al estado original. Por lo tanto, el CTI debe contar con un plan de contingencia para mitigar los efectos de un desastre, y que permita de forma rápida restablecer las funciones.

Con el fin de garantizar controles que aseguren la integridad, la totalidad, la exactitud, la autorización, la permanencia, así como la revisión y supervisión de los controles para promover el uso correcto y eficiente de los recursos y facilitar el logro de los objetivos de la institución, surge la necesidad de crear una herramienta que sirva como parámetro para asegurar el control y la seguridad del centro de tecnología de información de la Junta de Pensiones.

La implementación del Centro de Gestión tiene como propósito además de ser una instrumento de control, cumplir con normas establecidas; las cuales son documentos técnicos que contienen especificaciones técnicas de aplicación voluntaria, son elaborados por consenso de las partes interesadas ya sean fabricantes, administradores, usuarios y consumidores, centros de investigación, asociaciones entre otros y están basados en los resultados de la experiencia y el desarrollo tecnológico que son aprobados por el organismo internacional de normalización.

Las normas utilizadas como fundamento para el desarrollo del Centro de Gestión son la norma ISO 9001, la cual señala los requisitos para un sistema de gestión de la calidad que pueden ser utilizados por una organización para aumentar la satisfacción de sus clientes al cumplir sus requisitos y por las disposiciones legales obligatorias que sean aplicables; la norma ISO 19011, la cual proporciona orientación sobre los fundamentos de la auditoría, la gestión de los programas de auditoría, la conducción de auditorias de los sistemas de gestión de la calidad y ambientales, así como las calificaciones para los auditores de los sistemas de gestión de la calidad y ambientales;además de la norma ISO 9004 la cual señala las directrices para la mejora del desempeño utilizando como base la norma ISO 9001.

El cumplimiento de estas normas contribuirá a satisfacer los requerimientos; aplicar eficazmente la herramienta; alcanzar la mejora continua y la actualización de documentación y procesos según las necesidades y nuevos requerimientos del CTI.

Una vez definido el modelo propuesto debe ser avalado y aprobado por el Comité de Informática de la Junta de Pensiones y luego su aprobación final se da por parte de la Dirección Ejecutiva y Junta Directiva, así como su correspondiente divulgación y consideración dentro de la planeación de la institución.

CAPÍTULO III: MARCO METODOLÓGICO

METODOLOGÍA PARA LA REALIZACIÓN DEL DIAGNÓSTICO

1. Tipos de Investigación

1.1 Investigación Exploratoria

De acuerdo con Fernández, Hernández y Baptista: (2003:115)
"Los estudios exploratorios se efectúan, normalmente, cuando el objetivo es examinar un tema o problema de investigación poco estudiado o que no ha sido abordado antes. Es decir, cuando la revisión de la literatura reveló que tan solo hay guías no investigadas e ideas vagamente relacionadas con el problema de estudio" ; además añade "los estudios sirven para familiarizarnos con fenómenos relativamente desconocidos."(2003:116)

La investigación exploratoria se utilizó para la definición del tema y las variables de estudio para conocer los aspectos en cuanto al nivel de seguridad, soporte y lo concerniente a planes de contingencia del CTI de la Junta de Pensiones.

1.2 Investigación Descriptiva.

Fernández, Hernández y Baptista (2003:118) establece que "En un estudio descriptivo se selecciona una serie de cuestiones y se mide o recolecta información sobre cada una de ellas, para así (válgase la redundancia) describir lo que se investiga". Además añade que "la investigación descriptiva busca especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice."(2003:119)

Una vez que se conocen los elementos generales del problema, se comprueba la necesidad de profundizar en el estudio, utilizando un método con el cual se precise la información y que se denomina investigación descriptiva.

La investigación descriptiva recoge y tabula los datos. En el presente caso, se emplea para analizar, clasificar e interpretar los datos que han sido agrupados en cada variable definida anteriormente por medio de la investigación exploratoria, con el propósito de comprender y llegar a la solución del problema. Se describe el campo de acción que es el CTI de la Junta de Pensiones, partiendo de la aplicación y análisis e interpretación de los datos obtenidos.

1.3 Investigación Aplicada

Para Ezequiel Ander Egg (1989:67-68)

"La investigación aplicada guarda fuerte relación con la investigación básica, pues depende de los descubrimientos y avances de la investigación básica y se enriquece con ellos. Se trata de investigaciones que se caracterizan por su interés en la aplicación, utilización y consecuencias prácticas de los conocimientos."

En este estudio dicha técnica se refleja en el Modelo propuesto el cual se ha desarrollado luego de la investigación y aplicación de la información adquirida, proporcionando así una herramienta que permita el control de la seguridad y calidad en cuanto a hardware y software, soporte y contingencia del CTI de la Junta de Pensiones.

2. Sujetos

Sujetos implica lo que Arellano (1990: 116) denomina como un "simple conjunto investigado. Llamemos así a lo que es un conjunto particular de unidades estadísticas, que ni ha sido concebido como población o universo, ni tampoco ha sido seleccionado como muestra de una determinada población."

La muestra es una parte de la población que el investigador selecciona a través de algún método de muestreo, con el fin de evaluar algunos elementos de la población y no todos. Miguel Gómez Barrantes (1998:9) menciona que "el uso del muestreo es un procedimiento más rápido y barato y, en ciertos casos el único posible..."

El tamaño de la muestra es definido con el fin de poder contar con un apoyo tanto en el momento de elaborar la investigación como la propuesta, pues da una visualización de cómo se está trabajando actualmente en el CTI; de esta forma, se determinan los requerimientos con los que se debe de contar.

Para realizar el presente estudio, se utilizan dos tipos de muestreo, el primero con el fin de recopilar información de personas calificadas, conocedoras de la situación y manejo de los diferentes aspectos de importancia para el estudio. El segundo para conocer el punto de vista de los funcionarios que hacen uso del servicio que brinda el CTI.

Con el fin de seleccionar la primera muestra se utiliza el tipo de muestreo no aleatorio, el cual permite según Carlos Quintana Ruiz, “la selección por conveniencia de los elementos de la muestra y la selección intencional o de juicio”. Además, el mismo autor señala que “la selecciona una persona con experiencia y conocimiento amplio de la población en estudio, con el propósito de lograr una muestra lo más representativa posible de la población.” (1993, pág 156).

Los sujetos son personas calificadas que laboran o tienen alguna injerencia en el área como lo son el Jefe del CTI, el Administrador de la Base de Datos y el

Encargado de Soporte Técnico. A continuación se detalla una descripción de las funciones de cada uno de ellos.

El Jefe del CTI brindará información acerca de los procedimientos y operaciones administrativas del CTI. Entre sus funciones se encuentran:

- Definir las políticas y estrategias de administración de los sistemas de información, procesos y recursos informáticos de la Junta de Pensiones.
- Administrar los recursos financieros y tecnológicos asignados al CTI.
- Desarrollar y establecer planes de contingencia.
- Fijar los parámetros para la adquisición de soluciones de soporte lógico (software) y físico (hardware) y en general, de contratación de servicios informáticos.
- Promover la capacitación continua de los funcionarios del CTI, en nuevas herramientas, versiones y tecnología en general, para satisfacer los requerimientos de los proyectos.
- Coordinar con los demás Departamentos y Comité de Informática, el desarrollo de nuevos proyectos, la modificación y mantenimiento de los sistemas actuales y la fijación de las prioridades.
- Planificar y presupuestar la actualización de versiones de las herramientas de desarrollo y administración de la base de datos, así como herramientas complementarias.
- Realizar las acciones para el pago de las licencias de mantenimiento y soporte preventivo, para hacerle frente a cualquier tipo de contingencia que pueda afectar el buen desempeño institucional.

El Administrador de la Base de Datos suministrará información sobre el manejo y acceso a la información ya que es la persona responsable por la seguridad,

información clasificada y los datos compartidos almacenados en la base de datos. Tiene como responsabilidades:

- Velar por la seguridad de las bases de datos y analizar los archivos "log" para detectar errores, accesos indebidos, entre otros.
- Realizar tareas de mantenimiento de servidores y equipos de las bases de datos.
- Dar el acceso a los recursos de la base de datos previa autorización.
- Colaborar en la determinación de la metodología más adecuada de respaldo, para que la Base de Datos esté segura.
- Administrar el software original que permitirá la reinstalación de la Base de Datos en caso de ser necesario y suministrará una copia de respaldo para ser almacenada junto con el resto de las licencias de la Institución que custodia el CTI.
- Mantener actualizados los planes de recuperación de la Base de Datos.
- Probar la efectividad de los planes de recuperación de datos.

Encargado de Soporte Técnico el cual tiene el conocimiento detallado de los recursos de hardware y software con los que cuenta el CTI y tiene como funciones:

- Generar respaldos de archivos de la base de datos.
- Realizar las copias de respaldo de la información y procesos de cómputo que se llevan a cabo en el CTI, conforme con los parámetros preestablecidos.
- Instalar el "hardware" y el "software" que se adquiera. En el caso de equipo nuevo, configurar e instalar el software de manejo institucional.

- ❖ Llevar registros de fallas, problemas, soluciones, acciones desarrolladas, respaldos, recuperaciones y trabajos realizados.
- ❖ Aplicar en forma estricta las normas de seguridad y control establecidas.

Para la selección de la segunda muestra se utiliza la definida por Miguel Gómez Barrantes como "Aleatoria o al azar, es decir, dándole a cada uno de los elementos de la población una probabilidad conocida de ser incluido en la muestra". (1998, pág 10).

Actualmente la población de la Junta de Pensiones del Magisterio es de ciento sesenta y un funcionarios; sin embargo, sólo noventa y seis hacen uso de los sistemas de información, a éstos se restan los tres funcionarios calificados por lo que la población por utilizar como referencia es de noventa y tres funcionarios. Al usar un nivel de confianza de noventa y cinco y un error de punto quince se genera una muestra de veintinueve funcionarios, que son elegidos de una lista en orden alfabético utilizando un salto de tres. Estos hacen uso de la información como recurso en el quehacer diario o bien para la toma de decisiones y darán a conocer su perspectiva en lo que corresponde a la seguridad del CTI, la protección de la información y el conocimiento acerca del Plan de Contingencia.

3. Fuentes de Información

Las fuentes de información son las vías que utiliza un investigador para obtener la información necesaria con el fin de desarrollar el estudio.

Existen dos tipos de fuentes de información: la primaria, es utilizada por el investigador cuando no existen los datos que requiere, por lo tanto, debe suministrar datos recopilados por él mismo.

Para el desarrollo del presente estudio es necesario utilizar fuentes primarias, con el fin de conocer cuál es el modo de operación y seguridad del CTI y de esta forma poder elaborar el Modelo propuesto para el Centro de Gestión; por medio de la entrevista, el cuestionario así como la observación de manuales y procedimientos del CTI.
La fuente secundaria es cuando ya existe la información, y ha sido recopilada y suministrada por otra(s) persona (s) o institución (es).

Con el propósito de recopilar los datos necesarios, se utilizaron las siguientes fuentes: libros con información referente al tema en estudio, revistas, artículos e información obtenida de la Red Internet.

4. Descripción de los Instrumentos

4.1 Entrevista

La entrevista según Miguel Gómez Barrantes consiste en una técnica en la cual "un entrevistador visita a la persona que tiene la información y la obtiene de ella a través de una serie de preguntas que vienen planteadas en un cuestionario o boleta, en la cual se anotan las respuestas". (1998, pág. 33)

Para el presente estudio se aplican tres entrevistas, la primera al Jefe del CTI, con el fin de obtener información acerca del proceso administrativo, manejo de la seguridad y documentación referente a procedimientos. La segunda al Administrador de la Base de Datos, con el fin de identificar los procedimientos referentes a la seguridad de la Base de Datos y manipulación de la información; la tercera se aplica al Encargado de Soporte Técnico para conocer las políticas y procedimientos utilizados en la adquisición de software y hardware, así como las características de equipo que se utiliza en el CTI y en la Institución.

4.2 Cuestionario

El cuestionario, según Hernández, Fernández y Baptista, es un instrumento que "consiste en un conjunto de preguntas respecto a una o más variables a medir. El contenido de las preguntas de un cuestionario puede ser tan variado como los aspectos que mida." (2003 pág 391)

Consta de dos clases de preguntas: las cerradas y las abiertas. Los mismos autores indican que:

" Las preguntas cerradas contienen categorías o alternativas de respuesta que han sido delimitadas. Es decir, se presentan a los sujetos las posibilidades de repuesta y ellos deben circunscribirse a éstas. Pueden ser dicotómicas (dos alternativas de respuesta) o incluir varias alternativas de respuesta", (2003:393) Añaden además que las "preguntas abiertas no delimitan de antemano las alternativas de respuesta, por lo cual el número de categorías de respuesta es muy elevado; en teoría, es infinito." (2003, pág 396)

Para efectos del presente estudio se aplica un cuestionario de treinta y tres preguntas a veintinueve funcionarios de la Institución, lo que va a permitir hacer una comparación de lo que están percibiendo los usuarios del CTI contra lo que se está brindando, además del conocimiento que tienen acerca de las políticas y procedimientos que deben aplicar.

4.3 Análisis de Contenido

El análisis de contenido es conceptualizado por Ander-Egg, como "…una técnica de información que permite estudiar el contenido manifiesto de una comunicación, clasificando sus diferentes partes conforme a categorías establecidas por el investigador, con el fin de identificar de manera sistemática y objetiva dichas categorías dentro del mensaje."(1989, pág 327-336)

Además Hernández, Fernández y Baptista añaden que "es una técnica para estudiar y analizar la comunicación de una manera objetiva, sistemática y cuantitativa... una técnica de investigación para hacer inferencias válidas y confiables con respecto a su contexto."(2003, pág 413)

El análisis de contenido se desarrolla para el estudio de la práctica sana en lo que corresponde a hardware y software, soporte y contingencia; además de las Normas ISO que se utilizan en la elaboración de la propuesta, lo cual permite un mayor conocimiento para la interpretación de los datos según las normas y prácticas correctas.

4.4 Observación

La observación, según Marcelo Blanc,

" Consiste en la aproximación directa mediante los sentidos y la presencia física del investigador a los hechos y/o fenómenos que se desean estudiar."(1979, pág 45-54)

La observación brinda la oportunidad de completar y ratificar la información que anteriormente se ha recolectado por medio de otras técnicas o instrumentos.

Se realiza para la verificación de la documentación como: Plan de Contingencia, Manuales de Políticas y Procedimientos, documentación referente a respaldos. Además de observar el Área del CTI y de los servidores, revisión de los extintores y las rotulaciones.

5. Alcances

El proyecto se desarrolla en la Junta de Pensiones y Jubilaciones del Magisterio Nacional.

El estudio comprende las áreas de

- Soporte: Se consideran las políticas y procedimientos que se utilizan para brindar apoyo a las diferentes áreas y las que deben ser atendidas a nivel institucional por todos los usuarios.

- Seguridad de Hardware y Software
  - Seguridad física del equipo utilizado en la institución y el CTI (PC)
  - Servidores
  - Seguridad del entorno del CTI
  - Seguridad Lógica en lo que corresponde a manipulación y acceso a la información.
  - Motor de Base de Datos.

- Contingencia, que involucra lo correspondiente a las acciones por tomar en caso de alguna falla por causas provocadas por el hombre o bien naturales. (Plan de Contingencia)

Para la elaboración de la propuesta se utilizan las Normas ISO (Internacional Organization for Standardization).

ISO 9001:2000 "Sistemas de gestión de la calidad - Requisitos"

ISO 19011:2002 "Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental"

ISO 9004 "Sistemas de Gestión de la Calidad – Directrices para la mejora del Desempeño"

CAPÍTULO IV: ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

En este capítulo se desarrollan los diferentes pasos con el fin de realizar un diagnóstico del nivel de seguridad, soporte y lo concerniente a planes de contingencia del CTI. Tales pasos consisten en la recolección, codificación, tabulación, análisis e interpretación de los datos.

En cuanto se elige el diseño de investigación y la muestra que se va a utilizar, la etapa siguiente consiste en la recolección de los datos necesarios sobre las variables de la investigación.

Hernández Fernández y Baptista indican que

> " Recolectar datos implica: a) Seleccionar uno o varios métodos o instrumentos disponibles o desarrollados, tanto cuantitativos como cualitativos, dependiendo del enfoque del estudio, del planteamiento del problema y de los alcances de la investigación; b) aplicar el (los) instrumento (s), y c) preparar las mediciones obtenidas o datos levantados para analizarlos correctamente" (2003, pág 477)

1. Procedimientos existentes

El CTI cuenta con un manual de Políticas y Disposiciones Institucionales informáticas que contempla:

Disposiciones Generales: las cuales deben de cumplir todos los funcionarios. En ellas se hace referencia al uso de la identificación de usuario y palabra de paso, la frecuencia en que debe cambiarla; el uso de medios de almacenamiento de origen externo a la institución; el señalamiento a los departamentos para que desarrollen de forma periódica un perfil de cada uno de los usuarios para la correspondiente actualización de los roles; el uso del e-mail y computadoras, el respaldo de la información en forma periódica, el velar por el buen funcionamiento del equipo, el uso de software, la confidenciabilidad de la información y la

obligación de los usuarios a cerrar su sesión cuando no estén trabajando frente al computador, entre otros.
Disposiciones en el Análisis y Diseño de Sistemas: señalan las normas a las que se deben apegar las personas encargadas del desarrollo y mantenimiento de los sistemas.

Disposiciones de Seguridad: protegen el patrimonio de la institución y vinculan la obligación de crear un entorno de seguridad para sus trabajadores; los trabajadores por su parte, deben ayudar a respetar y tratar de cumplir estas disposiciones. Se establecen pruebas periódicas para la prevención de fallas tales como descargas eléctricas, control de incendios y prevención de fraude.

Disposiciones sobre la Base de Datos: estas deben ser acatadas por el Administrador de la Base de Datos para garantizar el buen funcionamiento de la Base de Datos y tratar de minimizar los riesgos de pérdida de información; entre ellos, procesos de respaldo y recuperación de la base de datos, registro de las actividades en las bitácoras correspondientes, la adecuada administración de los recursos y asignación de usuarios, por último las claves de acceso que se comunican al usuario por medio de un documento junto con las indicaciones para su utilización.

En cuanto al cumplimiento de las disposiciones antes mencionadas, actualmente en lo que corresponde a las disposiciones generales, se comunican algunas de ellas anualmente mediante una circular dirigida a todos los funcionarios; sin embargo, un 30% de los encuestados indica no conocer este documento, no obstante aplican algunas de las políticas mencionadas en el documento por iniciativa propia. Con respecto a las disposiciones de seguridad, estas son ejecutadas en un 90% por los usuarios ya que velan por la adecuada protección

de los bienes, recursos e información que se les han confiado, sin embargo, por desconocimiento es que no se ejecutan en su totalidad las políticas; mientras que los encargados las ejecutan en un 95%, pues realizan las tareas de respaldo, pruebas de los equipos UPS, mantenimiento preventivo al equipo de cómputo, no así al equipo de aire acondicionado ni a los detectores de humo. Para el cumplimiento de las disposiciones sobre la Base de Datos se cuenta con un documento el cual lleva el control y registra la fecha en que se realiza el respaldo, el tipo de respaldo realizado (FULLEXPORT, FULL UNIX), en qué servidor se realiza, la hora en que se ejecutó y en qué dispositivo fue almacenado (cinta de 4mm u 8mm); además de un campo de observación donde se puede anotar algún tipo de error o problema que haya evitado la finalización de forma satisfactoria del respaldo. El registro de cada uno de los respaldos indica el usuario que lo realizó y su firma. Aunado a esto se lleva una programación mensual de los respaldos por realizar en cada uno de los días; además de los procesos que corresponden a la asignación de usuarios y claves, así como las pruebas para la recuperación de la información.

Las tareas de soporte se canalizan por medio de órdenes de trabajo en las cuales se especifica la tarea que se solicita y el visto bueno de la jefatura, por lo que los encargados una vez que la realizan llevan como control un detalle. Además, en algunos casos se ha capacitado a un grupo selecto del personal de forma que puedan colaborar en el proceso, como lo es en el uso de las impresoras, errores en los programas o bien uso de los sistemas para que puedan identificar fácilmente la falla o bien puedan solucionar la dificultad.

El tiempo de respuesta en caso de alguna falla es muy variable pues depende en forma directa de la dificultad del problema, este puede durar desde unas horas hasta una semana; sin embargo, los usuarios consideran que es razonable el

tiempo de respuesta. Además un 70% señala que ha recibido capacitación tanto para el uso de los sistemas como en el equipo, por lo que pueden identificar en la mayoría de los casos si el problema se debe al hardware o al software.

2. Hardware y Software

El Centro de Tecnología de información cuenta con dos Servidores Sun, uno de ellos modelo Ultrasparc 170 de 187 MHZ con juegos de discos internos y externos, además de un tape backup interno de 4mm DDS2 y el otro, modelo Ultrasparc Enterprise 450 de 250 MHZ con juegos de discos internos solamente y un tape backup externo Sun Storedge L400 de 8 mm. El Ultrasparc 170 tiene instalado el sistema operativo Unix versión 2.50 de Solaris y con un motor de base de datos Oracle versión 7.3.2; el cual almacena la información de la institución de los primeros años. El Enterprise 450 fue instalado con el sistema operativo Unix versión 2.51 de Solaris y con un motor de base de datos Oracle versión 7.3.3, que guarda la información más reciente de la institución. Ambos equipos están protegidos por una UPS marca BEST de 5 KVA. También se cuenta con un servidor de correo interno administrado por el software de Microsoft Exchange y el Outlook en las máquinas de los usuarios.

Con respecto al modelo Enterprise, este equipo presenta algunas deficiencias ya que utiliza el software tanto de sistema operativo como de base de datos con el cual se compró, de forma tal que limita su rendimiento y administración en cuanto a controles de seguridad para los usuarios, así como el uso de las facilidades en la administración que ofrece el software más actualizado. En cuanto al modelo Ultrasparc 170 ya no cuenta con capacidad de crecimiento, limitando así su velocidad de transmisión, rendimiento y capacidad. La UPS actualmente presenta fallas en cuanto a batería por lo que se están buscando alternativas para sustituirla.

Actualmente se cuenta con una partida para la compra de servidores; sin embargo, no se ha podido hacer efectiva dado que existen aplicaciones que se encuentran desarrolladas en versiones que no son compatibles con la nueva tecnología disponible en el mercado. Por lo tanto el Comité de Informática aprobó desarrollo de un sistema de crédito y cobro para que se ponga en marcha al finalizar el presente año y de esta forma poder cambiar de plataforma.

Los computadores personales se caracterizan por contar con un procesador que va desde Pentium II de 64MB hasta Pentium IV de 512 MB, con disco duro en su mayoría de 40 GB y monitores de 15", exceptuando los del CTI que utilizan monitores de 21" en el Área de Desarrollo de Sistemas. Para la protección del equipo y la información, en su mayoría, los equipos están conectados a una UPS con regulador de voltaje en caso de falla del fluido eléctrico.

Actualmente los equipos Pentium II soportan en forma mínima las aplicaciones pues por su arquitectura en cuanto al procesamiento de datos, por la cantidad de sistemas y aplicaciones, se encuentran limitados para satisfacer los requerimientos de memoria y espacio. En cuanto a las UPS, según acuerdo emitido por la Junta Directiva todos los equipos deben de estar protegidos, de forma que se están adquiriendo para completar las faltantes, además por cada uno de los nuevos equipos se debe adquirir una UPS.

3. Factores de la seguridad física

Los riesgos en cuanto a la seguridad física del CTI se pueden clasificar en: acceso físico, incendio, inundación, fallas por fluido eléctrico, control de temperatura, aseo y mantenimiento; a continuación se detalla lo recopilado para cada uno de ellos.

Acceso Físico

En lo correspondiente al acceso al CTI, no existen sistemas de seguridad, dispositivos o personal que controle el acceso. Por este motivo todo el personal tiene libre acceso y no se ha instruido a los funcionarios sobre las en caso del ingreso de personal no autorizado. Además, se pudo observar que en el mismo piso donde se encuentra el CTI se encuentra ubicado el departamento de Relaciones Públicas, lo que provoca una entrada constante de personas ajenas no solo al CTI, sino a la institución.

La institución cuenta con un circuito cerrado de cámaras, pero estas se encuentran ubicadas en el área de las gradas, entradas principales de la institución y en el parqueo.

El acceso al área de servidores es restringido, ya que se encuentra en un área bajo llave que solo la tiene el encargado de soporte y el administrador de base de datos; además en caso de ingresar visitantes deben anotarse en un control o bitácora que registra el acceso e indica la fecha en que ingresó la persona, el número de cédula, el nombre, la hora de entrada, la hora de salida, la empresa, y el motivo por el cual tuvo que ingresar al área de servidores. Sin embargo, el Administrador de la Base de Datos señala que por lo general la gente se anota, pero en ocasiones no se respeta, por lo que considera que no es el control de ingreso más adecuado.

Se pudo observar que en la puerta de entrada tanto al Centro de Tecnología como a los servidores hay un rótulo que indica “Acceso Restringido” y en el caso de la puerta de los servidores hay un documento pegado llamado “Criterios por seguir para el Ingreso al área de los servidores” en el cual se identifican las

personas que cuentan con libre acceso, las que no requieren autorización previa, las que tienen acceso limitado y las personas que tienen acceso custodiado.

Incendio

El edificio donde se encuentra ubicado el Centro de Tecnología de Información es resistente al fuego, además los marcos de las puertas y las ventanas del CTI están fabricadas de aluminio; sin embargo, los muebles de cada uno de los módulos están fabricados de madera.

Como medida de prevención de incendios en el CTI se encuentran distribuidos tres extintores manuales de fuego debidamente señalados, dos tipo B (líquidos inflamables: gasolina, aceite y grasas) y C (equipo electrónico, corto circuito, instalaciones eléctricas); uno de ellos ubicado en el área de servidores y el otro en la entrada del CTI; el tercer extintor es tipo A (combustibles ordinarios: madera, papel, tela, plásticos) el cual se encuentra ubicado en la entrada al CTI. Actualmente sólo un miembro del CTI está capacitado para hacer uso de los extintores, los demás funcionarios desconocen su forma de uso.

Se cuenta con detectores de humo, éstos se ubican solamente en el área de servidores del CTI. Además, no se realizan pruebas periódicas para cerciorarse de que los detectores se encuentren en buen estado ni de la alerta en caso de incendio.

Inundación

El riesgo de una inundación por fugas de agua, desbordamiento de tuberías, goteras, entre otros es nulo; en lo que corresponde a la tubería sólo existe en los baños y en caso de problemas, el agua fluiría por las gradas. Además, los servidores se encuentran a un nivel más alto del suelo y cuentan con rodines; en

el caso de las goteras por lluvias, el techo cuenta una cubierta térmica evitando así que el agua pase a través de ella y caiga en el CTI; sin embargo, se han tenido problemas con goteras procedentes del sistema de aire acondicionado en dos ocasiones que, por descuido de los mismos funcionarios, han dejado el regulador de temperatura a un nivel muy bajo, lo que ha provocado que la unidad y los ductos del sistema de aire se congelen y en el momento de descongelarse se esparce el agua por el techo, la cual ha caído en los pasillos y no en ningún equipo eléctrico, ni en servidores.

Además tanto los computadores como el equipo de cómputo ubicado en toda la institución, se encuentra colocado más arriba del nivel del suelo, lo cual fue avalado por los usuarios de la institución.

Fluido Eléctrico

Para proteger la información en caso de que existan problemas con el fluido eléctrico, se utilizan UPS con regulador de voltaje para los computadores, tanto los que están ubicados en el CTI como en la mayoría de los equipos de los usuarios de la institución y fuente de poder interna para los servidores. Además, el equipo se encuentra conectado a tierra como medida de protección contra rayos.

El CTI cuenta con lámparas de emergencia en caso de que se corte el fluido eléctrico en lo que es la parte de iluminación, para no tener problemas a la hora de ingresar al cuarto de servidores y cerrar las aplicaciones y demás equipos. Se cuenta con una batería de 5 KVA que es suficiente para soportar ambos servidores, sin embargo, está teniendo problemas de batería, además la instalación eléctrica es independiente; dentro de la habitación, también están

conectados a esta batería, los routers, módems de líneas dedicadas y los switchs que interconectan.

Actualmente se cuenta con un pararrayos en la Institución, además en los edificios de los alrededores también hay, los cuales están ubicados más alto. Por ejemplo, el Templo Votivo al Corazón de Jesús, en de los edificios de la Corte y hay varios árboles cerca.

Control de temperatura

Para el control de temperatura se cuenta con aire acondicionado para todo el Centro de Tecnología de Información y con un ducto para el área de los servidores, pero no es suficiente para mantener una temperatura adecuada en la habitación, ya que es un cuarto bastante caliente; sin embargo, hasta el momento no ha presentado ningún problema con los equipos.

Aseo y Mantenimiento

Se cuenta con un lugar específico para almacenar la papelería y suministros de oficina dentro del CTI. En lo correspondiente al consumo de bebidas y alimentos no se permiten dentro del área de servidores; sin embargo, este hábito no se restringido a los puestos de trabajo.

Para la limpieza, el equipo de los servidores se moviliza fuera del área destinada con el fin de darle mantenimiento preventivo.

Una vez analizados cada uno de los factores de seguridad física, se presenta un resumen el que identifica los riesgos y la probabilidad de que ocurran, según la información suministrada.

Cuadro #1
Factores de Seguridad Física

	PROBABILIDAD	
	PORCENTAJE POSITIVO	**PORCENTAJE NEGATIVO**
Acceso Físico	46	54
Incendio	38	62
Inundación	100	-
Fluido Eléctrico	100	-
Control de Temperatura	-	100
Aseo y Mantenimiento	75	25

Fuente: Entrevista realizada a la Jefatura del CTI, Administrador de la Base de Datos, Encargado de Soporte Técnico y encuestas aplicadas a los usuarios.

El cuadro #1 muestra la probabilidad de que se dé una falla física que pueda poner en peligro tanto el buen funcionamiento del CTI como de la información. Entre los riesgos más latentes se encuentra el riesgo de falla en el equipo de los servidores debido a sobrecalentamiento; la posibilidad de que no se detecte un incendio a tiempo en el área del CTI, por falta de sistemas automáticos y la falta de revisión periódica de los detectores de humo ubicados en el área de servidores; por último el acceso físico, pues no se lleva un control que asegure el ingreso solo a personal autorizado al CTI. El riesgo menos latente pero de igual importancia es el que puede ser causado por mantenimiento o aseo del equipo; actualmente el fluido eléctrico e inundación están bien controlados, pero no se deben descuidar.

4. Factores para la protección de la información

Para identificar los factores para la protección de la información que utiliza el CTI éstos se pueden agrupar en: acceso a la información y manipulación de la información; a continuación se detalla lo recopilado para cada uno.

Acceso a la Información

La Junta de Pensiones ha establecido como política que cualquier usuario debe contar con clave de acceso para ingresar a la red institucional; esto es controlado por medio del sistema operativo; además una vez aquí validado debe volverse a identificar para accesar la información de la base de datos y por ende el ingreso a los sistemas.

El Administrador de la base de datos es el encargado de realizar la asignación y autorización de los accesos a la base de datos, asignando la identificación del usuario y la palabra de paso. La identificación del usuario se conforma por la primera letra del nombre y el primer apellido, en los casos que sea necesario se utiliza además la primera letra del segundo apellido; la palabra de paso es alfanumérica, sin una secuencia definida, al menos de nueve caracteres sin lógica alguna, para obligar al cambio de la contraseña que se brinda.

Para la creación de un nuevo usuario se debe emitir una orden de trabajo por parte de la jefatura interesada indicando los datos personales, el sistema en el que va a trabajar y las funciones que va a ejercer el nuevo usuario dentro del sistema. El administrador de base de datos elabora un documento al funcionario indicando el usuario de oracle y la palabra de paso, señala que la palabra de paso es confidencial y que el sistema monitorea de forma automática cada una de las acciones realizadas por el usuario en el sistema, además detalla la forma en que debe cambiar la palabra de paso, ejemplificando los pasos que debe seguir en el proceso. Sin embargo, el administrador de base de datos manifiesta, que a pesar de entregar un documento a los usuarios donde se señala el uso de su clave, muchos de ellos hacen caso omiso a esta recomendación y se ha detectado que en ocasiones han ingresado con el usuario de algún compañero que se encuentra incapacitado, de gira o de vacaciones.

Todos los funcionarios que hacen uso de los sistemas cuentan con una contraseña para ingresar a la computadora y en su mayoría tienen la posibilidad de cambiar la contraseña en caso de que se necesite. Un 40% de las personas encuestadas no recibieron ningún documento que le indicara el usuario y clave con las cuales podía hacer uso de los sistemas, estas personas tienen más de cuatro años de laborar en la institución. Mientras que el restante 60% recibió un documento; si bien un 28% de estos tiene más de cuatro años de laborar en la institución, sólo tienen de uno a tres años de desempeñar el puesto en el cual se ha requerido el uso de los sistemas.

Con el fin de concientizar a los usuarios de los riesgos que puede originar el préstamo de sus contraseñas, se emite un documento adicional al entregado con la clave de acceso, en donde se le recuerda a los funcionarios que deben cambiar su contraseña periódicamente y que no debe ser revelada a nadie, esto por medio de una circular que se emite anualmente por el CTI. Un 70% de los encuestados no tiene conocimiento de la existencia de este documento. El restante 30% lo conoce porque fue distribuido en el área de trabajo o bien debido a sus funciones propias, ya que reciben la correspondencia.

A pesar de las intenciones por parte del CTI de hacer conciencia en los usuarios, un 40% de ellos ha revelado su identificación de usuario y contraseña de acceso a los sistemas o del equipo.

Entre las herramientas que puede utilizar el CTI para promover el cambio de contraseñas, están las características propias del sistema operativo que tiene la posibilidad de obligar al usuario a cambiar la contraseña cada mes, de forma que tenga que elegir una nueva que no puede ser igual a las utilizadas anteriormente; por falta de recurso humano, no se ha configurado para que luego de una

cantidad de intentos fallidos inactive la clave o bien inactivarla en un tiempo determinado. Con respecto al control de contraseñas para el acceso a la base de datos, existe la limitante de la versión que se encuentra instalada actualmente, ya que no cuenta con la posibilidad de forzar al usuario a realizar el cambio de su palabra de acceso.

Manipulación de la información

Para la manipulación de la información, los usuarios una vez que cuenten con acceso a los sistemas, tienen restringidas las opciones del menú de acuerdo con su puesto y funciones de forma tal que dependiendo de su trabajo puedan manipular la información y así puedan agregar, modificar y borrar información por medio del sistema en la base de datos de la institución.

Además del controlar las claves de acceso, se controla el acceso a la información de la base de datos por medio de roles, definidos por el administrador de la base de datos, los cuales restringen al usuario a no tener control total de la información, al igual que las opciones del menú, donde, si el rol asignado al usuario no tiene derecho a una opción, esta no aparecerá entre las opciones.

Entre los privilegios más comunes están los de consulta, inserción, modificación y eliminación de datos. Otros privilegios que son menos comunes son los de creación de tablas e índices, los cuales son de uso restringido para usuarios que ejecuten procesos batch para la actualización de la información en forma masiva.

Como se mencionó, se ha detectado el ingreso al sistema de personas que se encuentran incapacitadas, de vacaciones o que se encuentran de gira. Esto hace que la asignación de roles pierda el motivo por el que son utilizados, puesto que no controla quién accesa la información, en forma confiable. Los usuarios

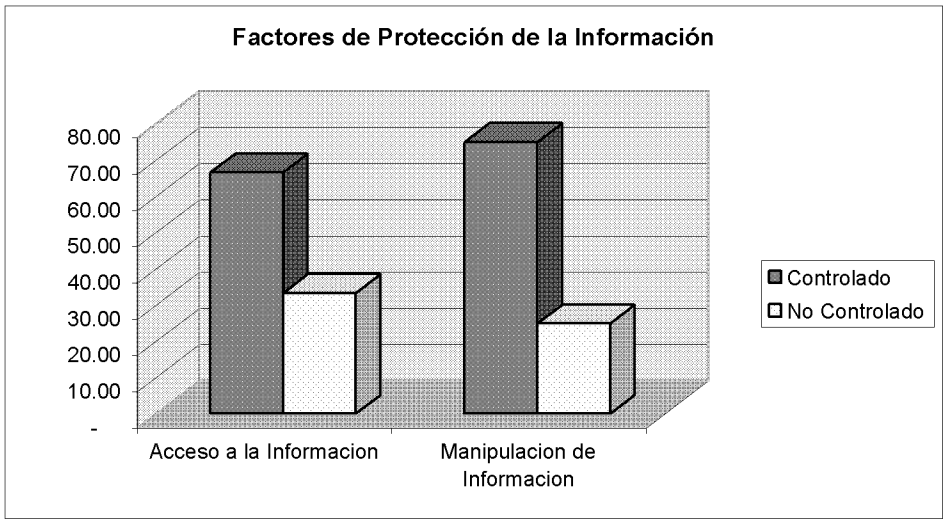
comparten sus claves ya que es más sencillo el pedir la contraseña del compañero ausente a elaborar una orden de trabajo y que su jefe de Área la autorice para la realización del cambio por el Administrador de la Base de Datos en la base de datos.

Otro aspecto que se observó es que muchos usuarios dejan sus sesiones abiertas a la hora de ir a almorzar o dejar su puesto de trabajo por alguna otra razón, lo que provoca que cualquier otro compañero utilice el usuario para manipular información; el administrador de la base de datos señala al respecto que se intentó controlar esta situación por medio de una propiedad que tiene la base de datos, de forma que, luego de cierto tiempo se elimine, la sesión, pero se presentaron algunos inconvenientes pues al ejecutarse eliminaba la conexión con el sistema operativo, y los usuarios no podían ingresar de nuevo, sino después de una hora, por lo que se eliminó esta propiedad. Sin embargo, la propiedad que se activó fue que un usuario sólo pudiera abrir hasta cuatro sesiones simultáneas en la base de datos y así controlar los recursos de conexiones al servidor, ya que en muchas ocasiones un solo usuario tenia hasta diez sesiones abiertas de las cuales solamente tres eran las realmente utilizadas. Además, los usuarios pueden abrir varias sesiones al mismo tiempo en equipos diferentes por lo que no se puede validar que el usuario que está conectado al computador sea el mismo que utiliza los sistemas o hasta con una clave de un compañero diferente.

Dentro de estas políticas institucionales se encuentra la revisión de medios de almacenamiento externo a la institución con el fin de eliminar la posibilidad de que contengan virus informáticos y no poner en peligro la información de la Institución, lo cual es ejecutado por un 60% de los funcionarios.

Una vez analizados cada uno de los factores para la protección de la información, se presenta un resumen el cual identifica los riesgos y la probabilidad de que ocurran, según la información suministrada.

Gráfico #1



Fuente: Entrevista realizada a la Jefatura del CTI, Administrador de la Base de Datos, Encargado de Soporte Técnico y encuestas aplicadas a los usuarios.

El gráfico #1 muestra el nivel de control que se ha realizado para proteger la información, lo que señala que tanto en acceso de información como en manipulación de información se han realizado tareas que permiten evitar el riesgo de alteración. En su mayoría las deficiencias se deben a la versión del equipo de base de datos, pues no se cuenta con herramientas que permitan fortalecer el acceso a la información, las cuales sí poseen las versiones actuales.

5. Políticas actuales para enfrentar Contingencia

El plan de contingencia para el CTI contempla documentación relacionada con administración de riesgos, recursos de riesgo, procedimientos de emergencia que deben aplicar en caso de una eventualidad, procedimientos de recuperación en caso de una catástrofe ya sea de índole natural o malintencionado, dicho

documento considera las áreas críticas de la institución a nivel de tecnología de información.

El plan de contingencia cuenta con un análisis para la estimación del valor de la pérdida y la estimación de la probabilidad de ocurrencia por tipo de amenaza (fuego, humo y gases, inundación entre otros) y por recurso (servidor, computador, sistemas, entre otros).

Además posee un plan de emergencia, en el cual se especifican las tareas por ejecutar en caso de una contingencia, primero señala cómo identificar la contingencia: se debe aplicar la prioridad sobre los recursos, luego según el tipo de contingencia sea poco severo, severo o muy severo se indican los pasos por seguir, se realiza un análisis del suceso en el cual se deben ejecutar las medidas correctivas y preventivas de lo sucedido y por último se debe documentar el evento; en caso de ser necesario señala que el plan puede ser modificado. El personal tiene conocimientos de los procedimientos por seguir en caso de una emergencia de incendio, inundación, terremoto, corte de fluido eléctrico, igualmente conocen las salidas de emergencia.

También cuenta con información de las personas de soporte interno y externo a las que se puede acudir en caso de una emergencia, entre la información se indica el nombre, el número de teléfono, el puesto y el comité al que pertenece sea del comité de informática, salud ocupacional o bien de la Dirección Ejecutiva y del CTI. En caso de ser externo se indica la empresa y el recurso al cual da soporte. En su mayoría el personal tiene conocimiento de la existencia del comité de salud ocupacional, así como de sus integrantes.

Como anexo se encuentra un diagrama que identifica la distribución de hardware de la institución, además de un diagrama de red en los edificios y la lista de hubs.

Se especifica además, los procedimientos de recuperación para volver al estado normal de operación de acuerdo con el tipo de falla, ya sea por fluido eléctrico, inundación, movimiento sísmico, fuego, acciones mal intencionadas y los recursos a los cuales afecta con su orden de prioridad; además se especifica el orden de prioridad para la recuperación de cada uno de los sistemas.

En este documento está especificada una revisión anual; sin embargo, no ha sido aprobado, por lo que las revisiones correspondientes no se han realizado. Esto provoca que la información no sea cien por ciento confiable, ya que muchos procedimientos que se especifican podrían haber variado con el tiempo.

En caso de falla del equipo de servidores, existe un contrato de mantenimiento preventivo y correctivo. El contrato indica que en días hábiles en menos de cuatro horas deben brindar respuesta a la emergencia. Sin embargo, el contrato cubre todos los días del año, por lo que fines de semana se debe contactar al soporte externo para que solucione el problema en caso de una falla de hardware. El resto del equipo, como por ejemplo los switch, routers o módems de líneas dedicadas del ICE, no están en un contrato, por lo que en caso de un problema se debe recurrir a otros medios de corrección.

Dentro del plan, el CTI también considera las posibles amenazas sobre los recursos, se definen actividades por realizar tanto por el personal como por el responsable de la ejecución; sin embargo, por el hecho de aún no haber sido aprobado no se señala explícitamente el nombre de las personas responsables de la ejecución de cada una de las tareas.

Se han determinado los tiempos críticos de demora o de servicio interrumpido y el impacto económico y de imagen que pudiera ocasionar la interrupción total o parcial de los servicios por lo que una vez realizados los estudios se determinó por parte de la Dirección Ejecutiva que por un problema dado, los servicios pueden estar interrumpidos hasta por ocho horas.

Se han adoptado las medidas de prevención precisas para garantizar la disponibilidad de los recursos necesarios para la recuperación de los datos. Como primer paso se cuenta con un plan de respaldo y se revisa anualmente el proceso de recuperación, de forma que se toma una de las cintas de respaldo para ejecutar el procedimiento de recuperación y verificar que esté correcto; este trabajo es realizado por una empresa externa dado que no se cuenta con capacidad para bajar el respaldo en la misma institución en coordinación con el administrador de la base de datos, la jefatura del CTI, el encargado de soporte y la auditoría interna. También se debe dar continuo mantenimiento preventivo a las unidades de respaldo y se revisa las bitácoras de los respaldos para verificar que se haya realizado bien.

Todo el esquema de seguridad se basa en el proceso de respaldo que se utilice, pues si se cuenta con un respaldo adecuado, pase lo que pase se puede recuperar la información, por lo demás se trata de disminuir riesgos con tener UPS, mejor ambiente alrededor del servidor y revisar aspectos ambientales.

A nivel de usuario, la mayoría no realiza respaldos frecuentes de la información que es relevante y vital en su quehacer diario, lo que provocaría la pérdida total de los archivos en caso de una contingencia.

6. Factibilidad Económica

El CTI cuenta con un Plan Anual Operativo (PAO), en el cual se describen cada una de las actividades como lo son los sistemas de información por desarrollar, cambios tecnológicos previstos, los recursos, los plazos y presupuesto asignado. Este se encuentra por escrito y es aprobado por la Dirección Ejecutiva. El CTI se encuentra a nivel de Staff, cuenta con la jefatura, un administrador de base de datos, secretaria, dos funcionarios para soporte técnico, siete analistas programadores los cuales dada la cantidad de proyectos y mantenimientos son recursos que la mayoría del tiempo realizan las tareas del día a día y no se pueden dedicar en forma completa al desarrollo de nuevas aplicaciones por lo que se les limita la posibilidad cumplir con todos los requerimientos de la institución.

La formulación del Presupuesto se realiza por parte de la Jefatura del CTI en coordinación con el analista asistente de la Jefatura. El cual se eleva para la aprobación a un comité conformado por jefaturas del CTI, Departamento Financiero Contable, CTI y Dirección Ejecutiva, para ser formalizado en la Junta Directiva.

Dentro del presupuesto se consideran partidas para pago de gastos que involucran los salarios, honorarios, viáticos, transporte, capacitación entre otros; un rubro correspondiente a mobiliario y equipo el cual es de aproximadamente que involucra el equipo de oficina; otro de los rubros es el de equipo especializado por la suma aproximada de millones, éste se utiliza para el cambio del cableado de la red, cintas de respaldo, compra de servidor de internet, compra de servidor de respaldo y otros equipos especiales que se requieran en el CTI; se cuenta con una partida alrededor de trescientos mil para la adquisición de

literatura; otra de las partidas es para construcción por la suma aproximada de millones para remodelación del área; y por último una partida de intangibles en la cual se encuentra la adquisición de software, licencias, migración de base de datos y sistema operativo por una suma aproximada de . Aunque no figure dentro del presupuesto en forma directa una partida para la seguridad del CTI, se puede contar con la partida para equipo especializado o bien la de intangibles. Sin embargo, en caso de ser necesario y dada la prioridad, se puede solicitar una modificación a otra partida, como actualmente se está haciendo para la compra de UPS y unidad de respaldo; además la jefatura del CTI se encuentra anuente a crear una partida para la seguridad o bien a apoyar mejoras.

La institución cuenta con el Comité de Informática, en el cual se debaten los asuntos informáticos que afectan a toda la organización; participa en la fijación de prioridades de los proyectos informáticos y aprueba los procedimientos estándares del CTI. El Comité de Informática está conformado por nueve miembros, los cuales pertenecen a distintas áreas y departamentos; por lo que en caso de implantar o modificar algún proyecto se debe contar con el visto bueno de este comité.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

El presente capítulo expone los resultados obtenidos producto del diagnóstico realizado en el capítulo anterior.

Éste se encuentra dividido en conclusiones y recomendaciones según la variable en estudio.

Conclusiones

Las conclusiones no son algo aparte, externo al análisis interpretativo. Al contrario, constituyen lo medular del mismo, es aquella parte en la que el investigador, considerando los resultados del análisis de los datos, se aboca a dar respuesta al problema planteado en la investigación.

Según Arellano,

> "Los informes in extensos normalmente ofrecen las conclusiones bajo título aparte, en forma puntualizada, y ya no tan atada a los datos concretos, Sin embargo, ellas no son algo esencialmente aparte del análisis interpretativo.
> Constituyen más bien su núcleo central, el lugar donde se atan todos los cabos, donde se ofrece una respuesta a las preguntas planteadas por el problema, y con ello se cierra el ciclo investigativo" (1990, pág 163).

Además, Gallardo agrega "las conclusiones se siguen mediante la articulación o cotejo de los resultados expuestos en el cuerpo central del informe con los objetivos de la investigación... Conocimientos que se siguen firmemente del material estudiado y que se expresan clara, concisa y, si es posible ordenadamente". (1998,pág, 205-206)

De la evaluación realizada y la recolección de los datos obtenidos, se puede concluir lo siguiente:

1. Procedimientos existentes

El CTI cuenta con un manual de políticas y disposiciones institucionales, el cual se encuentra por escrito y contempla las disposiciones de uso general para todos los funcionarios, disposiciones para el análisis y diseño de los sistemas, de seguridad que protegen el patrimonio de la institución, de base de datos para garantizar el buen funcionamiento y continuidad de operaciones.

Las disposiciones generales no se han comunicado de la mejor manera ya que no se aplican en su totalidad o algunas son aplicadas por iniciativa propia de los usuarios.

En lo que corresponde a las políticas de seguridad no se evidencia un adecuado mantenimiento del equipo de aire acondicionado ni de los detectores de humo, las restantes políticas se cumplen en forma satisfactoria.

Se cuenta con procedimientos y políticas para brindar soporte, las cuales se aplican según lo especificado.

2. Hardware y Software

El CTI cuenta con dos servidores Sun, un Ultasparc 170 y un Ultrasparc Enterprise 450, los cuales no brindan el mejor rendimiento o desempeño que ofrecen los equipos modernos en cuanto a su arquitectura. Además el Ultrasparc 170 ya no cuenta con capacidad de crecimiento.

El Software utilizado por los servidores se encuentra desactualizado limitando así su rendimiento y administración de la información.

La limitante que ha evitado realizar la migración de base de datos, es la existencia de dos aplicaciones no compatibles con las versiones actuales. Sin embargo por parte del comité de informática ya existe un acuerdo para que las aplicaciones sean desarrolladas en una versión más reciente y compatible para la migración.

El equipo con que cuentan los usuarios va desde Pentium II de 64MB hasta Pentium IV de 512MB; sin embargo, los Pentium II no soportan en forma satisfactoria las aplicaciones requeridas.

Existe un acuerdo de Junta Directiva en el que se encuentran anuentes a brindar protección de la integridad de los equipos, por lo que todos deben contar con su respectiva UPS.

3. Factores de la Seguridad Física

Acceso Físico

El CTI no cuenta con sistemas, dispositivos o personal de seguridad que controlen el acceso. Sin embargo, en la institución se encuentran ubicadas cámaras de circuito cerrado.

Tanto la puerta de entrada al CTI como a los servidores se encuentra rotulada e indica que el "Acceso es restringido"; en el área de servidores se especifica quiénes pueden entrar y bajo qué condiciones. Sin embargo, dado que el CTI se encuentra ubicado en el mismo piso que el Departamento de Relaciones Públicas provoca una entrada constante de personas ajenas tanto al CTI como a la institución.

El acceso al área de servidores es restringido dado que se encuentra bajo llave; sin embargo, no se lleva un control adecuado del ingreso ya que en ocasiones no se anota en la bitácora.

Incendio

El peligro de una eventualidad por incendio es mínimo ya que tanto el edificio como los marcos de las puertas y ventanas donde se encuentra ubicado el CTI son resistentes al fuego; sin embargo, los muebles de los módulos están fabricados de madera. Para aminorar el riesgo en el CTI se encuentran distribuidos tres extintores manuales de fuego debidamente señalados, dos tipo B y C y uno tipo A; sin embargo, solo un funcionario del área conoce cómo utilizarlo.

Sólo en el área de servidores se cuenta con detectores de humo; sin embargo, no se realizan pruebas periódicas de su estado.

Inundación

La probabilidad de una inundación por fugas de agua, desbordamiento de tuberías o goteras es nulo. Pero se han presentado irregularidades con el sistema de aire acondicionado dado que los ductos se han congelado y en el momento de descongelarse se ha esparcido el agua por el techo y ha caído a los pasillos.

Los servidores y el equipo tanto del CTI como de la institución se encuentran colocados a un nivel más alto del suelo.

Fluido eléctrico

Tanto en el CTI como a nivel institucional se cuenta con UPS, regulador de voltaje y fuente de poder interna para los servidores, los cuales se encuentran conectados a tierra como medida de protección contra rayos. Se cuenta con una batería de 5 KVA que es suficiente para soportar ambos servidores; sin embrago,

está teniendo problemas en la batería, además la instalación eléctrica está independiente dentro de la habitación. También se conecta a la batería los routers, módems de líneas dedicadas y los switchs que protegen los dispositivos que son indispensables para la comunicación de la institución.
En el CTI se encuentran ubicadas lámparas de emergencia. Además se cuenta con pararrayos ubicado en el techo de la institución y en los edificios ubicados en los alrededores.

Control de temperatura

Aunque el área de servidores se encuentra dentro del CTI éste no recibe la adecuada temperatura dado que los ductos no están bien colocados, por lo que se mantiene la temperatura en el área del CTI, pero no en el área de servidores, lo cual presenta un riesgo significativo en los equipos.

Aseo y Mantenimiento

El riesgo de una eventualidad debido al aseo, es muy bajo, ya que se procura en la mayoría de los casos cumplir con las disposiciones para este fin.

En cuanto al mantenimiento del equipo se realiza para los servidores de manera preventiva.

4. Factores para la protección de la información

Acceso a la Información

Se tiene como política que todo usuario cuente con una clave de acceso para ingresar a la red institucional y otra para accesar la información de la base de datos la cual es asignada por el administrador de base de datos, según las especificaciones creadas para este fin; además éste hace entrega de un

documento donde se indica el usuario y la palabra de paso, los cuidados en cuanto a confidencialidad y la forma en que se debe cambiar la clave.

Aunque existen políticas referentes al uso de la clave de acceso y en su mayoría se le ha comunicado a los usuarios, algunos hacen caso omiso y en ocasiones utilizan la clave de otro compañero cuando este no se encuentra. Sin embargo, en su mayoría las personas conocen el documento que se emite cuando se entrega la clave. En procura de evitar estas negligencias el CTI emite anualmente una circular donde se recuerda el cambio de las claves periódicamente; sin embargo, esta no ha sido divulgada de la mejor manera pues son muy pocos los que conocen el documento y lo ponen en práctica.

El CTI se encuentra limitado para usar las características que ofrece el sistema operativo para la inactivación de la clave, ya que no cuenta con recurso humano para realizar la configuración.

En cuanto al control para el acceso a la base de datos, existe la limitante de la versión que se encuentra instalada actualmente, ya que no cuenta con la posibilidad de forzar al usuario a realizar el cambio de su palabra de acceso.

Manipulación de la Información

Para la manipulación de la información los usuarios cuentan con la clave de acceso para ingresar a los sistemas y dentro de los sistemas tienen opciones restringidas por medio del menú, según las tareas que realiza.

Además se controla el acceso a la información de la base de datos por medio de roles los cuales son definidos por el analista de sistemas y creados en la base de datos por el administrador de la base de datos.

Los privilegios más utilizados son los de consulta, inserción, modificación y eliminación de datos; existen otros privilegios como son creación de tablas e índices para usuarios especializados que ejecutan procesos.

Una deficiencia en el uso de las claves es que muchos usuarios dejan sus sesiones abiertas cuando no están en su sitio de trabajo y cualquier otro compañero puede realizar operaciones con el usuario ya abierto. Por lo tanto, se han hecho intentos por controlarlo; sin embargo, se presentaron inconvenientes con la conexión del sistema operativo.

Dado que los usuarios acostumbraban tener muchas sesiones abiertas, aunque no todas las esté usando, se restringió el acceso a cuatro sesiones simultáneas en la base de datos y así se controlan los recursos de conexiones al servidor.

En su mayoría los usuarios revisan la existencia de virus en los dispositivos externos, por lo que cumplen con las disposiciones para este fin.

5. Políticas actuales para enfrentar Contingencia

El plan de contingencia para el CTI es un documento bastante completo pues especifica los riesgos, los recursos, los procedimientos, los valores de pérdida, estimación de probabilidades, plan de emergencia, anexo de la distribución del hardware de la institución y diagramas de red, las tareas por seguir, los datos de las personas que pueden colaborar en caso de una emergencia; por último señala los procedimientos de recuperación dependiendo del tipo de falla.

Sin embargo, a pesar de contar con todo un Plan de Contingencia este no se encuentra aprobado, ni se le han realizado las revisiones que según el mismo documento está estipulado debe ser cada año.

En lo que corresponde a fallas en los servidores se cuenta con un contrato de mantenimiento preventivo y correctivo, este contrato cubre todos los días del año. El resto de los equipos como los switch, routers o módems de líneas dedicadas del ICE, no están dentro de un contrato.

Se han realizado estudios por parte de la Dirección Ejecutiva y se ha determinado que el tiempo de servicio interrumpido puede ser de hasta ocho horas.

Para garantizar la disponibilidad de la información en caso de una eventualidad, se ha dado mantenimiento al equipo de respaldo, se lleva un control en bitácora y se han realizado pruebas para la recuperación, éstas se realizan anualmente por una empresa externa en coordinación con el personal del CTI y la auditoría interna. En lo que corresponde a respaldos de la información relevante a nivel de usuario, éstos no lo realizan frecuentemente por lo que en caso de eventualidad se perderían.

6. Factibilidad Económica

El CTI cuenta con un Plan Anual Operativo (PAO), en el cual se describen cada una de las actividades como lo son los sistemas de información por desarrollar, cambios tecnológicos previstos, los recursos los plazos y presupuesto asignado. Se encuentra por escrito y es aprobado por la Dirección Ejecutiva.

La formulación del Presupuesto se realiza por parte de la Jefatura del CTI, el cual se eleva para la aprobación a un comité conformado por la Jefatura del CTI, departamento Financiero Contable y Dirección Ejecutiva, para ser formalizado en la Junta Directiva

El presupuesto contempla diferentes partidas, entre las más relevantes se considera la de equipo especializado y la partida de intangibles en la cual se encuentra la adquisición de software, licencias, migración de base de datos y sistema operativo. Aunque no figure dentro del presupuesto en forma directa una partida para la seguridad del CTI se puede contar con la partida para equipo especializado o bien la de intangibles. Sin embargo, en caso de ser necesario y dada la prioridad se puede solicitar una modificación a otra partida ya que existe anuencia por parte de la jefatura en apoyar mejoras en este campo.

La institución cuenta con el Comité de Informática en el cual se debaten los asuntos informáticos a nivel institucional, por lo que en caso de implantar o modificar algún proyecto se debe contar con su visto bueno.

Recomendaciones

Las recomendaciones son las indicaciones de acción que el investigador aconseja llevar a la práctica, como consecuencia de los hallazgos del estudio.

> Arellano agrega "Aquellas investigaciones que se llevan a cabo para resolver un problema de tipo práctico, naturalmente concluyen haciendo 'recomendaciones de acción'… Lo mismo ocurre con las investigaciones de tipo evaluativo (aquellas que evalúan instituciones, programas). También ellas concluyen con una serie de 'recomendaciones', derivadas del diagnóstico evaluativo logrado." (1990, pág, 167)

Según indica Gallardo "Son sugerencias del autor del informe acerca de futuras tareas que se desprenden del conocimiento aportado en las conclusiones o de las dificultades que para su obtención se pusieron de relieve en la discusión". (1998,pág, 206)

1. Procedimientos existentes

Se recomienda realizar una campaña de divulgación utilizando el servidor de correo con el fin de dar a conocer las disposiciones generales a todo el personal, de forma que se le haga llegar a los usuarios la información de las políticas como documento completo y enviar recordatorios cada mes de manera selectiva, para que se vaya tomando conciencia y sean ejecutadas.

En cuanto al mantenimiento preventivo del aire acondicionado y de los detectores de humo, se debe cumplir dicha política; por lo que se recomienda que lo antes posible se realice la revisión, dado que pone en peligro la continuidad de las operaciones en caso de una eventualidad.

2. Hardware y Software

Se recomienda la adquisición de un servidor que tenga características de redundancia en el hardware tal como doble fuente de poder, además de manejar un arreglo de discos duros utilizando RAID5. Sería conveniente que contara con al menos dos procesadores para agilizar el tiempo de respuesta y memoria RAM de 1GB para brindarle mayor cantidad de memoria a la memoria compartida de la base de datos.

En cuanto al software de sistema operativo y base de datos se recomienda instalar las ultimas versiones, Solaris 9 en lo que corresponde a Sistema Operativo y Oracle 9i Release2 en Base de Datos y mantener un contrato de mantenimiento correspondiente a actualizaciones hasta donde sea posible y evitar así su desactualización.

En lo que corresponde a la información que se almacena en los servidores se recomienda hacer una integración para que toda la información quede en el nuevo servidor, dejando al servidor Enterprise 450 como un espejo del nuevo servidor que se utilice en primera instancia como servidor de desarrollo y a la vez como servidor de respaldo en caso extremo. Utilizar el servidor Ultrasparc 170 tal y como está, en forma independiente del nuevo servidor, con las aplicaciones que no son compatibles temporalmente hasta que sean desarrolladas en una versión más reciente y que esto no sea un obstáculo para atender la recomendación.

En cuanto a la UPS de los servidores se recomienda la compra de un equipo de mayor capacidad y características tales como conexión de baterías en cascada para aumentar la capacidad en caso de ser necesario, cambio de baterías en

caliente para evitar la suspensión del servicio de la UPS a los servidores lo que evitaría el tener que apagar los servidores en caso de mantenimiento.
Se recomienda cambiar el equipo Pentium II se recomienda por equipos más modernos y aumentar así el desempeño de los usuarios, y estos equipos utilizarlos en procesos menos pesados como trabajos secretariales que solo requieran procesadores de texto u hojas electrónicas y cuando se requiera para alguna donación.

Se recomienda seguir atendiendo el acuerdo de Junta Directiva donde se pronuncian acerca del uso de UPS en todos los equipos, como se ha realizado hasta la fecha.

3. Factores de la Seguridad Física

Acceso Físico

Se recomienda la instalación de dispositivos y sistemas de seguridad que monitoreen el acceso al CTI y que se pueda identificar la persona que ingresa, así como llavines eléctricos que puedan configurarse para abrir el dispositivo con el carné del funcionario, logrando que el CTI permanezca siempre cerrado. Además de una cámara de circuito cerrado para darse cuenta de quien ingresa y sale del cuarto de servidores ya que no en todos los casos se anota la persona que ingresa. También se debe realizar el registro en bitácora cada vez que alguien ingresa, ya que es una norma que se debe acatar.

Con respecto a compartir el piso con el departamento de Relaciones Públicas se recomienda el traslado de ese departamento a otro piso o bien realizar una redistribución, para independizar el ingreso del CTI y de esta forma reducir de manera considerable el tráfico de personas.

Incendio

Se debe capacitar a todo el personal del CTI en la forma adecuada de extinguir un incendio y el correcto uso dependiendo del contenido del extintor.

Se deben realizar pruebas periódicas de los detectores de humo en el cuarto de servidores para tener la seguridad de que en caso de una eventualidad, dará señal de alerta y la instalación de otros detectores en el CTI. Además de la instalación de pulsadores manuales que avise al personal que el edificio debe evacuarse, para evitar daños al personal en otros pisos.

Inundación

Se recomienda mantener una temperatura adecuada constante en los sistemas de refrigeración para evitar que la unidad se congele y se produzcan goteras a través de los ductos que cubren al CTI.

Fluido eléctrico

En lo que corresponde al fluido eléctrico se recomienda continuar con los procedimientos actuales para seguir garantizando la integridad y protección de los equipos y por ende de la información.

Control de temperatura

Se recomienda adquirir una unidad adicional de aire acondicionado para el cuarto de servidores que mantenga la temperatura adecuada para los equipos y el que se encuentra actualmente utilizarlo para los equipos del área del CTI y el ambiente.

4. Factores para la protección de la información

Acceso a la Información

Una vez implementadas las recomendaciones en cuanto a hardware y software del punto A, se recomienda utilizar todas las ventajas que brindan estas herramientas en el manejo y control de usuarios.

Luego realizar una evaluación en cuanto al uso de la clave, se debe tomar un acuerdo si continúan dándose irregularidades, de forma tal que si un funcionario utiliza el usuario de un compañero que no se encuentre en la institución, ambos reciban una amonestación por el mal uso del acceso a la información y poner en peligro su integridad.

Manipulación de la Información

Se recomienda utilizar las ventajas que brinda el nuevo software de sistema operativo y base de datos para que se controle el tiempo que un usuario pasa ocioso dentro del sistema, economizando los recursos de la base de datos y brindando un mejor rendimiento.

5. Políticas actuales para enfrentar Contingencia

Dadas las ventajas en cuanto a la información que suministra el plan de contingencia, se recomienda que sea aprobado y mantenerlo actualizado, realizando las revisiones anuales según lo estipulado.

En cuanto al respaldo de la información de los equipos personales de los funcionarios, se recomienda brindar la capacitación necesaria para que ellos mismos sean capaces de respaldar sus archivos y liberar al CTI de esa tarea.

6. Factibilidad Económica

Se recomienda seguir los actuales procedimientos velando que se cumplan tal y como se hace hoy en día, con el fin de brindar un crecimiento informático a nivel institucional.

CAPÍTULO VI: PROPUESTA

INTRODUCCIÓN

Con el fin de brindar respuesta al problema de la presente investigación se propone la elaboración de un documento en donde se especifiquen los aspectos que se deben considerar para la implementación de un Centro de Gestión en el Centro de Tecnología de Información de la Junta de Pensiones y Jubilaciones del Magisterio Nacional, utilizando como base las normas ISO 9001:2000 "Sistemas de gestión de la calidad requisitos", ISO 19011:2002 "Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental", ISO 9004 "Sistemas de Gestión de la Calidad – Directrices para la mejora del Desempeño"

El Centro de Gestión constituye una comisión o área que apoya la actualización y mejoramiento de los procesos de seguridad, soporte y contingencia que se realizan en el Centro de Tecnología de Información; y en conjunto con el Comité de Informática apoya el desarrollo informático Institucional.

Este documento tiene como objetivo asegurar la estandarización de los procesos operativos, promover la coordinación de actividades y la ejecución de una gestión eficiente y de mejora continua que garantice un mejor servicio al cliente interno y externo.

POLÍTICAS INTERNAS PARA LA OPERACIÓN DEL CENTRO DE GESTIÓN

- Adoptar e implementar las políticas y directrices técnicas emitidas por el CTI, Comité de Informática, la Dirección Ejecutiva y la Auditoría Interna.
- Realizar actividades técnicas con la participación activa de los involucrados, para impulsar el aseguramiento de la Calidad en el CTI.
- Establecer canales efectivos de coordinación de actividades con la Dirección Ejecutiva, el Comité de Informática, CTI y Auditoría Interna.
- Establecer a nivel interno normas de seguridad para el hardware y software y cumplir con las definidas por la Auditoría de Interna, el CTI y las contenidas en los manuales técnicos respectivos.
- Establecer y procurar el mejoramiento continuo y el aseguramiento de la calidad del CTI.

RELACIONES DE COORDINACIÓN

El Centro de Gestión Informática, para realizar un trabajo eficiente, debe establecer mecanismos de coordinación y comunicación a nivel interno, que garanticen la integridad y efectividad en la operación del hardware y software.

Las principales relaciones de coordinación que debe mantener el Centro de Gestión son con: la Dirección Ejecutiva, Auditoría Interna, el CTI, Comité de Informática y usuarios.

EQUIPO DE TRABAJO DEL CENTRO DE GESTIÓN

La comisión o área estará conformada por un grupo interdisciplinario de funcionarios, los cuales en conjunto deben reunir los siguientes atributos personales: ético, de mentalidad abierta, diplomático, observador, perceptivo, versátil, tenaz, decidido y seguro de sí mismo.

Contar con conocimientos acerca sistemas de gestión, aplicación del sistema de gestión, normas de sistemas de gestión de la calidad, métodos y técnicas relativas a la calidad, procedimientos aplicables u otros documentos que indiquen la práctica sana en lo correspondiente a gestión de la calidad; conocimientos para comprender el contexto tecnológico en el cual se desenvuelve el Centro de Tecnología de Información y por ende el Centro de Gestión; conocer la institución para poder comprender el entorno, cultura organizacional y haber trabajado para la institución al menos un año.

Con el fin de que el equipo de trabajo sea más competente y nivelar su conocimiento se brindará capacitación en lo referente a Centros de Gestión y Calidad, la cual se realizará durante seis meses en diferentes temas de estudio, los cuales brindarán retroalimentación a los otros compañeros del equipo de trabajo. Se estima para la capacitación un monto de $3.000.00 que incluyen alrededor de doce cursos.

Según el Boletín Informativo Nosotros y la Calidad N° 4 señala:

> "De nada serviría una documentación perfecta sin un equipo humano comprometido con una ejecución transparente, competente, innovadora y de calidad, en el marco de un ambiente amable y de armónica convivencia." (2001, Diciembre) De http:// caribe.udea.edu.co/new/main/pdf/sgc/boletin_calidad/BOLETIN_CALIDAD_No_4.pdf

ADOPCIÓN DE NORMATIVA TÉCNICA

El Centro de Gestión Informática para el desarrollo de su gestión en lo que concierne a seguridad, soporte y contingencia cuenta con documentación técnica de acatamiento obligatorio que respalda los procesos que desarrolla. Estos documentos son:

- Manual de Políticas y Disposiciones Institucionales informáticas, que establece normas técnicas relativas al desarrollo informático, de cumplimiento en todos los niveles de la organización según corresponda, con el fin de contar con uniformidad, calidad en la prestación de los servicios, comunicación adecuada y racionalidad en la utilización de las herramientas y equipos. Contempla las disposiciones generales, las cuales deben ser acatadas por todos los funcionarios; disposiciones de Análisis y Diseño de Sistemas donde se señalan las normas a las que se deben apegar las personas encargadas del desarrollo y mantenimiento de los sistemas; disposiciones de Seguridad que protegen el patrimonio de la institución y vincula la obligación de crear un entorno de seguridad para sus trabajadores; las disposiciones sobre la Base de Datos deben ser acatadas por el Administrador de la Base de Datos para garantizar su buen funcionamiento.
- Documento para solicitud de servicios de soporte. (Ordenes de Trabajo).
- Plan de Contingencia para el CTI. Contempla documentación relacionada con administración de riesgos, recursos de riesgo, procedimientos de emergencia que se deben aplicar en caso de una eventualidad, procedimientos de recuperación en caso de una catástrofe ya sea de índole natural o malintencionado. Dicho documento considera las áreas críticas de la institución a nivel de tecnologías de información.
- Plan Anual Operativo, en el cual se describe cada una de las actividades por desarrollar por la Institución y tiene como objetivo impulsar un proceso sistemático equitativo y gradual de desarrollo de sistemas de información, que apoye los procesos de planificación, programación, dirección, vigilancia, monitoreo, control, evaluación y toma de decisiones a nivel institucional.
- Plan Estratégico de la Institución, en el cual se visualiza el horizonte de la institución, definiendo objetivos y estrategias para conseguirlo.

Como documentación de referencia:

- Norma ISO 9001 "Sistemas de Gestión de la Calidad Requisitos", como apoyo en la implementación del Centro de Gestión.
- Norma ISO 19011 "Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental", como apoyo en la implementación del Centro de Gestión.
- Norma ISO 9004 "Sistemas de Gestión de la Calidad – Directrices para la mejora del Desempeño"
- Documentación que haga referencia a la práctica sana en cuanto a seguridad del CTI.

ESTRUCTURA

Para definir el programa del Centro de Gestión y así lograr los sus objetivos, se propone la estructura que permita visualizar los procesos operativos, mediante programas, subprogramas y actividades por realizar; lo que ayuda a delimitar de forma clara el alcance y tareas para cada uno de los programas en el proceso de iniciación del Centro Gestión y su posterior mejoramiento e inclusión de otros programas para las otras áreas del CTI así como en un futuro de toda la Institución.

En la estructura se establecen tres programas para la presente propuesta:

- Seguridad de hardware y software
- Soporte Técnico
- Contingencia

Seguridad de Hardware y Software

La información y los recursos informáticos: equipo, programas y datos, son activos que deben ser protegidos del acceso no autorizado, la manipulación y la destrucción; además de brindar al cliente interno y externo equipo y software que pueda responder a sus necesidades de forma oportuna y precisa, utilizando tecnología de punta para soportar el quehacer institucional.

Su desarrollo se refiere a la seguridad física del equipo que se encuentra en el CTI y en la institución, de forma que se fomenten las medidas de control orientadas a la continuidad de operaciones y al aseguramiento de la calidad del servicio, además del cumplimiento efectivo de las políticas establecidas.

En cuanto a la seguridad lógica, dado que los recursos son compartidos por un gran número de personas físicamente dispersas, se hace necesario establecer controles garantizando que su acceso se realiza de acuerdo con el nivel jerárquico y funciones del personal de forma que se proteja la integridad de la información.

Soporte Técnico

Mediante la implementación de este programa se genera el desarrollo de la metodología de trabajo que permita una administración eficiente de los equipos ubicados en el CTI, así como los que se encuentran ubicados en la institución.

El programa considera la formulación y ejecución de planes para el mantenimiento preventivo y correctivo de los dispositivos (aire acondicionado y detectores) y del hardware disponible en el CTI; así como velar por el cumplimiento de las disposiciones generales correspondientes a la plataforma técnica y estándares institucionales, los cuales deben ser de dominio común a nivel institucional y como apoyo para la adquisición y contratación de hardware.

Planes de Contingencia

El desarrollo de este programa contempla la orientación, elaboración y actualización del plan de contingencia, con el fin de minorizar el impacto y promover la continuidad de operaciones en caso de una eventualidad; según las políticas establecidas por el CTI para este fin y mejoras que la práctica sana establezca.

ACTIVIDADES

Seguidamente se detalla cada una de las actividades que contiene la estructura para el Centro de Gestión Informática. Antes de establecer las actividades por realizar dentro de los programas, se debe modificar o actualizar las áreas involucradas, con el fin de brindar un servicio en las óptimas condiciones y de esta forma procurar y mantener un mejoramiento continuo.

SEGURIDAD DE HARDWARE Y SOFTWARE

Para promover el mejoramiento continuo y la calidad en cuanto al hardware y software para el manejo de la base de datos, se debe adquirir un servidor que tenga características de redundancia en el hardware tales como, doble fuente de poder para que en caso de que una de las dos falle, la otra mantenga trabajando el equipo mientras se repara la dañada ya que evitaría la caída del servidor abruptamente, además de manejar un arreglo de discos duros utilizando RAID5 con cambio de discos en caliente lo que evitaría que en caso de que un disco duro falle se vaya a perder la información almacenada. Sería conveniente que contara con al menos dos procesadores para agilizar el tiempo de respuesta y memoria RAM de 1GB para brindarle mayor cantidad de memoria a la memoria compartida de la base de datos. Un equipo con estas características tiene un costo de $7.684.00 I.V.I.

En cuanto al software de sistema operativo y base de datos se recomienda instalar las ultimas versiones, Solaris 9 en lo que corresponde a Sistema Operativo y Oracle 9i Release2 en Base de Datos y mantener un contrato de mantenimiento correspondiente a actualizaciones hasta donde sea posible y evitar así su desactualización. El Solaris 9 se encuentra incluido en la compra del equipo de base de datos y con respecto a Oracle se mantiene un contrato que da a la institución el derecho de actualizar las versiones tanto de desarrollo como de administración de datos, el costo del contrato anual es de $12.622.38, el cual se encuentra dentro de los costos fijos de operación de la institución.

Para poner en funcionamiento lo anterior se debe realizar un proceso de Migración de Base de Datos el cual consistiría en integrar toda la información contenida en los servidores al nuevo servidor, dejando al servidor Enterprise 450 como un espejo del nuevo servidor que se utilice en primera instancia como servidor de desarrollo y a la vez como servidor de respaldo en caso extremo. Se debe usar el servidor Ultrasparc 170 tal y como está, en forma independiente del nuevo servidor con las aplicaciones que no son compatibles con las versiones que se utilizarán, como lo es la versión de desarrollo en carácter de Oracle, temporalmente hasta que sean desarrolladas en una versión más reciente y que esto no sea un obstáculo para iniciar la migración.

El desarrollo de la migración debe estar a cargo del Administrador de Base de Datos, con el apoyo y coordinación de la Dirección Ejecutiva y el Centro de Tecnología de Información, dado que es un proyecto de impacto institucional. Además se debe contar con asesoramiento tanto para la configuración del servidor como para la migración de la base de datos, colaboración de los analistas de sistemas y usuarios externos. Lo anterior se propone para mejorar el desempeño de los programas de la institución, los controles de seguridad y

administración de la información, lo que implica un costo aproximado de ¢836.160.00. (empresa asesora)

En cuanto a la UPS de los servidores se debe adquirir un equipo de mayor capacidad y características tales como conexión de baterías en cascada para aumentar la capacidad en caso de ser necesario, cambio de baterías en caliente para evitar la suspensión del servicio de la UPS a los servidores, lo que evitaría el tener que apagar los servidores en caso de mantenimiento; tiene un costo de $4.792.00 I.V.I.

Para el control de acceso físico al CTI se deben instalar llavines de seguridad eléctricos que permitan el acceso de los colaboradores por medio del carné de la institución, registrando el día y hora en que ingresaron. En caso de personas externas a la institución, el acceso será con autorización de la secretaria la cual llevará un registro de los visitantes. El costo de dicho equipo, que permita el ingreso por medio de carné y registre a los funcionarios es de $3.200.00 I.V.I.

Para controlar el ingreso al área de servidores se propone la instalación de una cámara adicional al sistema de seguridad de la institución, que brinda vigilancia las 24 horas, con la cual, en caso necesario, se sabría quién hizo ingreso a dicha área. El costo de un sistema de circuito cerrado con un punto de control es de ¢330.762.87.

En cuanto a compartir el piso con el Departamento de Relaciones Públicas, se proponen dos alternativas, la primera sería el trasladar este departamento a otro piso, si es que existe actualmente un área donde pueda ser reubicado, esto a criterio de la Dirección Ejecutiva de la Institución. La otra es independizar la entrada al CTI cerrando el pasillo por el que se comunican ambos departamentos,

dejando la entrada al Departamento de Relaciones Públicas independiente. La movilización de paneles e instalaciones tendría un costo aproximado a un millón de colones.

Para proteger la información y el equipo del CTI en caso de incendios, se propone la instalación de diez detectores de humo en el área donde se encuentre el CTI y dos pulsadores de alarma para poder alertar a los funcionarios que están ubicados cerca del CTI o bien en otras áreas que se puedan ver afectadas.

Esto tendría un costo de $890.00 por los detectores y por las manijas de incendio $180.00. Además de capacitar a todo el personal del CTI en cuanto al uso de los extintores de fuego y su uso correcto según el contenido, el cual no tendría costo alguno dado que cuando el personal de los Bomberos hace los cambios de los extintores, estos dan la capacitación con los extintores que tienen que recargar, según la fecha de vencimiento.

Para mantener una temperatura adecuada para los servidores que sea independiente de la temperatura que puedan soportar los funcionarios del CTI, se debe instalar un sistema de enfriamiento independiente para esta área. El costo de un aire acondicionado independiente para el área de servidores es de ¢645.245.86.

Actividades del Centro de Gestión para el Programa Seguridad de Hardware y Software.

Procurar que los riesgos de una eventualidad por inundación o problemas con el fluido eléctrico, estén bien controlados como hasta la fecha. Además, velar por el

cumplimiento del mantenimiento preventivo de los equipos de acuerdo con la programación definida.

Revisar continuamente la bitácora de entrada al CTI con el fin de controlar el registro adecuado y que se apliquen procedimientos de respaldo, así como la bitácora de acceso a los servidores.
Velar para que la administración de la base de datos, se realice según metodologías y controles que permitan una operación eficaz y eficiente de los sistemas y aplicaciones; de forma que se aproveche al máximo las herramientas y facilidades que provee el software de Sistema Operativo (Solaris 9) y de Base de Datos (Oracle 9i Release2).

Promover que la administración del diccionario de datos, la cintoteca, los manuales técnicos de operación se revisen con frecuencia; además de mantener actualizada la documentación que respalda los sistemas y las aplicaciones, mediante la aplicación de métodos adecuados, que garanticen su vigencia e integridad.

SOPORTE TÉCNICO

El primer paso corresponde a la comunicación de las disposiciones informáticas por medio de una campaña de divulgación la cual debe ser realizada con la colaboración de la secretaria del CTI y utilizando como herramienta el correo interno de la institución. De esta forma se le hace llegar a los usuarios la información del documento completo y se envían recordatorios de manera selectiva, que correspondan a uso del equipo y de los sistemas cada mes, de manera que se cree conciencia a los usuarios de su responsabilidad y el debido uso de los recursos, sea hardware o software.

Como medida de control, luego de seis meses, se debe realizar una pequeña encuesta a los funcionarios para determinar si las disposiciones son conocidas. Por parte de los encargados de soporte, con el apoyo de la secretaria del CTI y del Administrador de la Base de Datos, según corresponda se realizará una verificación del cumplimiento de las mismas. Con las conclusiones de la encuesta y los resultados de la verificación, se deben tomar medidas más agresivas o bien conservar el mismo esquema.

Para cumplir con lo establecido en las políticas sobre el mantenimiento preventivo del aire acondicionado y de los detectores de humo, además como práctica sana se deben realizar las revisiones de los dispositivos por lo menos dos veces al año; éstas tienen un costo anual de ¢60.000.00 por la revisión de los detectores de humo y de ¢95.000.00 anual por el mantenimiento del sistema de aire acondicionado.

El equipo de los usuarios se debe procurar rotar los Pentium II, a trabajos livianos como son el manejo de procesadores de texto u hojas electrónicas o cuando se realice alguna donación y que la adquisición de los nuevos equipos sean Pentium IV con el fin de aumentar el desempeño, dado las aplicaciones que deben utilizar.

Actividades del Centro de Gestión para el Programa de Soporte

Brindar apoyo en la divulgación y controlar el cumplimiento de las políticas, normas y estándares informáticos institucionales, con el fin de verificar su cumplimiento y mantener uniformidad e integridad en el hardware y software utilizado.

Verificar el cumplimiento del mantenimiento de los detectores de humo y del aire acondicionado.

En caso de realizar alguna nueva conexión eléctrica, velar que se realice según las especificaciones establecidas para trabajos de este tipo.

En cuanto a la adquisición de equipo para los funcionarios debe supervisar que éste sea Pentium IV o superior.

Coordinar junto con el CTI el mantenimiento preventivo para el hardware y el software del CTI, en forma periódica con el fin de garantizar la eficiencia, eficacia y productividad de la gestión.

Coordinar junto con el CTI evaluaciones periódicas del rendimiento de hardware y software utilizado, para determinar los niveles de eficiencia, eficacia y satisfacción de los usuarios.

Participar en el análisis y recomendación de las ofertas presentadas para la adquisición o contratación de hardware, software y emitir el criterio técnico en conjunto con el CTI para que se garantice la operación efectiva de los procesos de trabajo.

PLANES DE CONTINGENCIA

Para que el Plan de Contingencia sea de apoyo en caso de una eventualidad, lo primero que se debe realizar es su actualización y aprobación por parte del Comité de Informática y la Dirección Ejecutiva. Una vez aprobado, se debe notificar y reunir a las áreas involucradas en el proceso, para que conozcan la forma de actuar, además de comunicar a todo el personal de la existencia del plan y del papel que juegan dentro de éste.

Actividades del Centro de Gestión para el Programa Planes de Contingencia

El CTI en conjunto con el Centro de Gestión debe realizar la revisión anual del Plan de Contingencia. Deben estar al pendiente de algún cambio en el personal responsable de las tareas en caso de siniestro; con el fin de comunicarle a la nueva persona su actividades dentro del Plan y modificar el registro de responsables. Además deben considerar si se producen cambios en el entorno informático que afecten el contenido y puesta en marcha del Plan.

Promover la realización de simulacros de emergencia para que el personal responsable de tareas se familiarice con su ejecución; además de propiciar una retroalimentación, en beneficio de la Institución.

El Centro de Gestión en coordinación con el CTI y con cada uno de los departamentos debe establecer los procedimientos alternativos para el funcionamiento ante la imposibilidad de utilizar los sistemas informáticos.

FUNCIONES PROPIAS DEL CENTRO DE GESTIÓN

El Centro de Gestión evidencia un compromiso de la Administración con una eficaz prestación de los servicios y del mejoramiento continuo, para que el Centro de Tecnología de Información brinde inicialmente servicios de calidad en cuanto a Hardware y Software, Soporte y Contingencia.

Para la definición de las funciones que debe realizar se utilizan como base las normas:

ISO 9001:2000. Sistemas de Gestión de la Calidad Requisitos.

ISO 9004. Sistemas de Gestión de la Calidad – Directrices para la mejora del desempeño.

- Dado que la Administración apoya la creación del Centro de Gestión, debe evidenciar su compromiso con el desarrollo e implementación:
  - Asegurando la creación de Objetivos de Calidad los cuales deben ser medibles considerando las necesidades actuales y futuras de la Institución, los niveles de satisfacción de las partes involucradas, estudios comparativos, entre otros; para conducir a la mejora del desempeño de la institución y de los programas que involucra el presente estudio.

  - Comunicando a la Institución acerca de la Política y Objetivos de Calidad y promoviendo la retroalimentación.
  - Solicitando informes acerca del funcionamiento del Centro de Gestión.
  - Procurando la disponibilidad de recursos para el Centro de Gestión con el fin de que pueda satisfacer las necesidades.

- Promover políticas y objetivos para incrementar la conciencia, la motivación y la participación activa de las personas en el proceso del Centro de Gestión.

- Elaborar procedimiento para la creación de documentos, que permitan normalizar la forma en como se confeccionan. Este procedimiento debe cubrir todos los documentos que se generen tanto en el Centro de Gestión como en el Centro de Tecnología de Información, entre ellos los procesos, disposiciones y metodologías.

- Elaborar un control de documentos que establezca la metodología para realizar la revisión, aprobación y actualización de los documentos del Centro de Gestión y del Centro de Tecnología de Información, de forma que asegure la existencia de la última versión de los documentos y que las actividades se

realicen según las disposiciones. Estas deben encontrarse en los puntos de uso y el Centro de Gestión debe custodiar un respaldo de los documentos y llevar un control maestro actualizado.

- Promover la utilización de los formatos de documentos y de control de documentos en el CTI.

- El Centro de Gestión debe identificar y analizar los procesos de cada uno de los programas y en caso de ser necesario promover cambios o mejoras. Además analizar si alguna de las áreas debe atender requisitos Legales o Reglamentarios.

- Analizar los procesos de cada uno de los programas e identificar el tipo de usuarios ya sean internos o externos con el fin de poder estudiar y cumplir con sus necesidades y documentarlos. Además, considerar los requisitos legales aplicables.

- Promover la creación de una Política de Calidad en coordinación con la Junta Directiva y Dirección Ejecutiva, la cual debe fundamentarse en la Misión y Visión de la institución, ser coherente con otras políticas y estrategias globales de la empresa, así como incluir una mejora continua en relación con la satisfacción de las necesidades y expectativas de los clientes y partes involucradas. La Política de Calidad debe ser revisada al menos una vez al año para mantener su continua adecuación.

- Establecer metas y estrategias para alcanzar los objetivos de calidad propuestos, además de revisar y aprobar la planeación de la calidad durante un año determinado.

- Para las adquisiciones de equipos se debe procurar que se definan e implementen procesos de compra con el fin de satisfacer las necesidades y requisitos, los cuales deben estar documentados; además de asegurarse que el producto adquirido cumple con los requisitos especificados.

- La Mejora Continua consiste en realizar revisiones periódicas al Centro de Gestión en el cual se evalúa el cumplimiento de la política y objetivos de calidad, las acciones correctivas y preventivas tomadas, los resultados de las revisiones anteriores y el análisis de oportunidades de mejora; con el fin de verificar que todas las actividades se cumplan según las disposiciones establecidas y determinar la eficiencia y eficacia del Centro de Gestión.

  Para realizar este proceso se puede hacer partícipe a una persona de la institución que no pertenezca al Centro de Gestión el cual puede ser asignado por la administración y junto con un representante del Centro de Gestión, para evaluar los conocimientos del o los candidatos de acuerdo con la preparación académica y conocimientos sobre Calidad. (Una vez que se le haya suministrado la información básica acerca de Calidad y Normas ISO).

  Las revisiones se deben calendarizar de forma que se realicen por lo menos una vez al año y que evalúen cada uno de los programas y la función del Centro de Gestión dentro de la institución.

  Como parte de la Mejora Continua se deben realizar encuestas de satisfacción de los usuarios tanto internos como externos, además de realizar grupos de discusión con los usuarios. De los resultados obtenidos se debe realizar un análisis (quejas, sugerencias, recomendaciones y hallazgos en general) para

así lograr identificar oportunidades de mejora, acciones preventivas y correctivas.

La Mejora Continua debe implicar:

Razón para la mejora: identificar el problema y la razón por la que se debe atacar.

Situación Actual: evaluar la eficacia y eficiencia del proceso que se está realizando e identificar la raíz del problema.

Posibles Soluciones: explorar varias alternativas de solución y realizar un análisis de estas para poner en marcha la que más se ajusta de acuerdo a la problemática según el programa.

Evaluación de los efectos: una vez atacado el problema se debe confirmar que sus efectos hayan disminuido y que la solución ha funcionado.

Implementación y Evaluación: se debe prevenir que el problema vuelva a suceder en la misma área o bien en otras áreas.

DETALLE DE COSTO Y CALENDARIZACIÓN DEL PROYECTO.

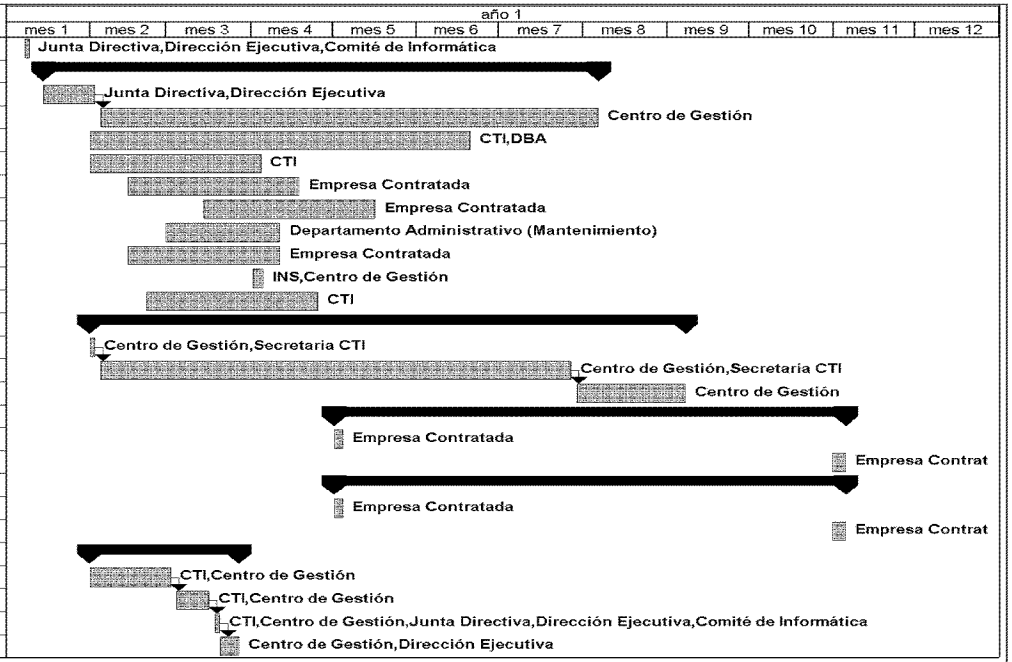
❖ Costos:

Puesta en Marcha de Centro de Gestión en el Centro de Tecnología de Información.
Cuadro de Costos

	Costo en $	Costo en ¢
Capacitación Equipo de Trabajo Centro de Gestión	$3,000.00	
Servidor de Base de Datos	$7,684.00	
Asesoría Externa para Migración de Base de Datos		¢836,160.00
UPS para servidores	$4,792.00	
Llavines de seguridad eléctricos	$3,200.00	
Cámara en el Área de Servidores		¢330,762.87
Distribución y movilización de Panels para la independencia del de D.R.P.		¢1,000,000.00
Instalación de diez Detectores de Humo en el CTI y dos pulsadores de incendio	$1,070.00	
Aire Acondicionado independiente para Area de Servidores		¢645,245.86
Mantenimiento Preventivo de Aire Acondicionado del CTI costo anual		¢95,000.00
Matenimiento Preventivo de Detectores de Humo costo anual		¢60,000.00
SubTotal	**$19,746.00**	**¢2,967,168.73**
Costo en Colones Tipo Cambio ¢440	¢8,688,240.00	¢2,967,168.73
COSTO TOTAL	**¢11,655,408.73**	

❖ Cronograma de Actividades:

Id	Nombre de tarea	Duración
1	Aprobación de la Puesta en Marcha del Centro de Gestión.	2 días
2	**Conformación del Equipo de Trabajo**	**146 días**
3	Elección del Personal del Equipo	15 días
4	Capacitación del Personal del Equipo	131 días
5	Adquisición de Equipo de Base de Datos y Migración de B.D.	100 días
6	Adquisición e Instalación de UPS para Servidores	45 días
7	Adquisición e Instalación de Llavin Eléctrico para la entrada del CTI	45 días
8	Adquisición e Instalación de cámara de vigilancia en el Área de Servidores	45 días
9	Movilización de Paneles para independizar el CTI.	30 días
10	Adquisición e Instalación de Detectores de Humo y manijas de incendio	40 días
11	Capacitación del uso de extintores de fuego	4 días
12	Aquisición e Instalación de Aire Acondicionado en el Área de Servidores	45 días
13	**Campaña de Divulgación Dispocisiones Informáticas**	**157 días**
14	Entrega de Dispocisiones a los usuarios	2 días
15	Recordatorios Mensuales	125 días
16	Realización de Encuesta sobre Dispocisiones informáticas	30 días
17	**Revisión / Mantenimiento de Detectores de Humo**	**134 días**
18	Primera	3 días
19	Segunda	3 días
20	**Revisión / Mantenimiento de Aire Acondicionado**	**134 días**
21	Primera	3 días
22	Segunda	3 días
23	**Actualización del Plan de Contingencia**	**39 días**
24	Revisión del Plan de Contingencia	22 días
25	Actualización del Plan	10 días
26	Aprobación del Plan	2 días
27	Notificación del Plan	5 días



Proyecto: Centro de Gestión para El CtI
Fecha: mié 21/07/04

Tarea · División · Progreso · Hito · Resumen · Resumen del proyecto · Tareas externas · Hito externo · Hito externo · Fecha límite

BIBLIOGRAFÍA

AENOR. *Conceptos Básicos.* Extraido el 15 Noviembre, 2003 de http://www.aenor.es/normaliz/frprnm01.htm

Ander Egg, Ezequiel. (1989). *Técnicas de Investigación Social.* Buenos Aires: Humánitas. (21° edición)

Arellano, J. (1990). *Elementos de Investigación. La investigación a través de su informe*. Editorial Universidad Estatal a Distancia, San José.

Biblioteca UDEA (2001, Diciembre). *Nosotros y la Calidad* N°4. Extraido el 15 Mayo, 2004 de http://caribe.udea.edu.co/new/main/pdf/sgc/boletin_calidad/BOLETIN_CALIDAD_No_4.pdf

Blanc, M. (1979). *Cómo Investigar.* Editorial Universidad Estatal a Distancia.

Consultores Profesionales en Informática, S.A. (1994). Copyright by AUDISIS, *Seminario en Informática, Modulo II Auditoría a la Seguridad de los Centros de Procesamiento de Datos*. San José de Costa Rica.

Contraloría General de la República. (1995). *Manual sobre normas técnicas de control interno relativas a los sistemas de información computadorizados* Primera Parte.

Delgado, X. (1998). *Auditoría Informática.* Editorial Universidad Estatal a Distancia.

Echenique, J.A. (1990). *Auditoría en Informática.* Editorial McGraw-Hill Interamericana de México, S.A.

EDPAA. (1994). *Manual de Revisión CISA: Dominio 4 Controles de Acceso Lógico Físico y Ambientales.*

EProm Access Basic Server. (Estudios y Programación). *Estructura del Manual de Calidad.* Extraido el 08 Marzo, 2004 de http://www.abserver.es/eprom/descarga/ est09.htm

Fine, L. (1988). *Seguridad en Centros de Cómputo Políticas y Procedimientos.* Editorial Trillas, S.A de C.V.

Freedman, A. (1993). *Diccionario de Computación* (5ta edición).

Gallardo, H. (1998). *Elementos de investigación académica.* Editorial Universidad Estatal a Distancia (13 reimp, de la 1era edición).

G&G Links SC Ingenieros Consultores (1995-2004). *Calidad.* Extraido el 10 Diciembre, 2003 de http://www.gglinks.com/ca.html.

Gómez, M. (1998) *Elementos de estadística descriptiva.* Editorial Universidad Estatal a Distancia. (1ra reimpresión, de la 3ra edición)

Hernández, R., Fernández, C & Baptista,P. (2003). *Metodología de la Investigación.* México. Editorial Mc Graw-Hill.

Homo quilitas *Asegúrese un futuro de Calidad. Norma ISO 9001:2000.* Extraido el 10 Diciembre, 2003 de http:// www.homoqualitas.com/castella/infos/iso90002000/ portada.htm.

Instituto de Normas Técnicas de Costa Rica. *Norma INTECO 2000-12-15 ITE-ISO 9001:2000 "Sistemas de gestión de la calidad requisitos"* . Primera Edición 2001

Instituto de Normas Técnicas de Costa Rica. *Catálogo del Programa Anual de Cursos y Seminarios.* Extraido el 18 Marzo, 2004 de http://inteco.or.cr/capacitacion.

Instituto de Normas Técnicas de Costa Rica y Proyecto CTCAP-China. (2001, Febrero*). La Normalización Técnica, Herramienta para la Competitividad*.

The Institute of Internal Auditors Research Foundation, (1991). *Systems Auditability and Control Report. Module 9 "Security"*.

ISO TC 176/SC 3 – ISO TC 207/SC 2 (2002, Febrero 13). *ISO/FSIS 19011:2002 (ES) "Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental"*

Ley del Sistema de Pensiones y Jubilaciones del Magisterio Nacional (2000) .

Manual de Repaso de Información Técnica para el Examen Cisa. Edición 2000. (décima).

MGS. *Introducción Conceptos Calidad.* Extraido el 10 Diciembre, 2003 de http://www.mgar.net/soc/intro

Moreno, Raúl. *La nueva versión de las normas ISO*. Extraido el 15 Noviembre, 2003 de http://raulalberto.tripod.com.co/paginadealimentos/id28.html

Municipio de Sabaneta (2003, Febrero 26). *Nuestro CompromISO con la Calidad. Boletín N° 4.* Extraido el 15 Mayo, 2004 de http://www.sabaneta.gov.co/web Sabaneta/control/doc/boletin%204.pdf

Norma Internacional. *Traducción Certificada ISO 9004 "Sistemas de Gestión de la Calidad – Directrices para la mejora del Desempeño".*

Nuevas Normas ISO 9000:2000. *Selección y uso de la tercerea edición de las normas ISO 9000. Documento: ISO/TC 176/N 613 (*2000, Octubre). Extraido el 15 Noviembre, 2003 de http://www.piqueras.org/qualitat/iso_sdpi/9000/normas.htm

Piattini, M. & Del Peso, E. (1998). *Auditoría Informática un enfoque práctico.* Alfaomega Grupo Editor, S.A. de C.V.

Quintana, C. (1983). *Estadística Elemental.* Editorial de la Universidad de Costa Rica.

Quintana, C. (1993). *Elementos de Inferencia estadística.* Editorial de la Universidad de Costa Rica. (1ra reimpresión)

Rodríguez, L.A. (1995). *Seguridad de la Información en Sistemas de Cómputo.* México. (1ra edición)

Royero, Jaim (2002, junio). *El control de Gestión*. Extraido el 15 Enero, 2004 de http://www.monografias.com/trabajos11/conges/conges.shtml.

Valdés, L.. (1993). *Conocimiento es Futuro.* México. Editorial Mc Graw-Hill.

ANEXOS

San Pedro, 16 de junio, 2004

Señores
ULACIT

Estimados señores:

La estudiante Angela Tencio Chacón me ha presentado para revisión de estilo el documento denominado "Aspectos que se deben considerar para la implementación de un Centro de Gestión en el Centro de Tecnología de Información de la Junta de Pensiones y Jubilaciones del Magisterio Nacional en lo que concierne a seguridad, soporte y contingencia utilizando la Norma ISO 9004 "Sistemas de Gestión de la Calidad – Directrices para la mejora del desempeño."

He revisado y corregido los aspectos referentes a estructura gramatical, acentuación, ortografía y puntuación, vicios de dicción que se trasladan al escrito y he comprobado que se han incorporado las correcciones al presente documento.

Por lo tanto, hago constar que se encuentra listo para ser presentado a la Universidad como trabajo de graduación.

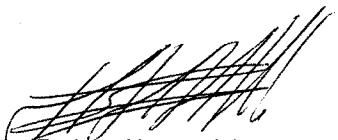
Atentamente,

M.Sc. Marianela Abellán Vargas
Filóloga
Carné 10702

San José, 24 de junio de 2004

Yo Rodney Herrera López como tutor del trabajo realizado por la Srta. Ángela Tencio Chacón y con el Título "Aspectos que se deben considerar para la implementación de un Centro de Gestión en el Centro de Tecnología de Información de la Junta de Pensiones y Jubilaciones del Magisterio Nacional, en lo que concierne a seguridad, soporte y contingencia utilizando la Norma ISO 9004: Sistemas de gestión de calidad – Directrices para la mejora del desempeño", luego de las revisiones del caso, doy por aceptado que dicho trabajo se encuentra listo para su respectiva defensa.

Atentamente,



Rodney Herrera López
Cédula 1-673-773
Tutor

ENTREVISTA AL JEFE DEL CENTRO DE TECNOLOGÍA DE INFORMACIÓN

Aspectos Administrativos.

¿Se realiza un plan operativo anual para el CTI ?

¿El plan operativo describe las actividades (sistemas de información a desarrollar, cambios tecnológicos previstos, los recursos y plazos necesarios)?

¿El plan se encuentra formalizado por escrito y aprobado por la Dirección?

¿Cuál es la estructura organizacional del CTI?

¿Esta estructura es necesaria y suficiente para el desarrollo de cada una de las actividades?

¿Quiénes intervienen en la formulación del presupuesto de la División de Informática?

¿Qué aspectos se consideran?

¿Existe la posibilidad de crear una partida para la seguridad del CTI?

¿Usted apoyaría la creación de mejoras en la seguridad del CTI?

¿Existe un comité de informática en el cual se debaten los asuntos informáticos que afectan a toda la empresa ?

¿En el comité informático se dan a conocer las necesidades del conjunto de la organización?

¿El comité de informática participa en la fijación de prioridades de los proyectos informáticos?

¿La división de informática participa activamente en los procedimientos estándares del CTI o estos son fijados por el comité de informática?

¿Cuenta el CTI con un procedimiento o política para la adquisición de bienes y servicios?

Plan de Contingencia.

¿Se cuenta con un plan de contingencia?
¿En dicho plan se consideraron las posibles amenazas sobre los recursos, se definen las actividades a realizar y se designaron a las personas encargadas de ejecutarlas?

¿Se han determinado los tiempos críticos de demora o de servicio interrumpido y el impacto económico y de imagen que pudiera ocasionar la interrupción total o parcial de los servicios?

¿Se han adoptado las medidas de prevención precisas para garantizar la disponibilidad de lo necesario para la recuperación de los recursos considerados críticos?

¿Se ha previsto en el proyecto algún plazo para la actualización del plan? ¿Cada cuánto tiempo?

¿Es de conocimiento de cada una de las partes involucradas?

Seguridad Física.

¿Existen sistemas de seguridad y/o personal que controle el acceso al CTI?

¿Todo el personal cuenta con libre acceso al CTI?

¿Se cuenta con dispositivos de seguridad para el acceso al CTI?

¿Se ha instruido al personal del CTI sobre qué medidas tomar en caso de que alguien pretenda entrar al CTI sin autorización?

¿Existe un control o bitácora que registre el acceso a los visitantes?

¿El CTI se encuentra ubicado en un edificio resistente al fuego?

¿Los muebles, las alfombras, las cubiertas de las ventanas del Centro de Tecnología son a prueba de incendios?

¿Se tiene asignado un lugar específico para la papelería y utensilios de trabajo?

¿Éste se encuentra fuera del CTI?

¿Existen detectores de humo instalados en el CTI?
¿Se hacen pruebas periódicas del funcionamiento de los detectores?

¿El personal del CTI cuenta con la capacitación necesaria en técnicas de extinción de incendios?

¿Existen extintores de fuego?

Manuales ( )
Automáticos ( )
No existen ( )

¿Están señaladas las zonas donde se encuentran los extintores y el tipo de contenido?

¿Cuentan con sistemas automáticos de extinción?

¿Existen dentro de las políticas, controles establecidos en el proceso de interrupción de energía en caso de incendio?

¿Se cuenta con pulsadores de alarma de incendios y su sonido se detecta en diferentes áreas como en los puestos de seguridad, localmente, entre otros?

¿Se cuenta con un drenaje adecuado en el área y alrededores del CTI?

¿Se prohíbe entrar al área con bebidas y alimentos?

Seguridad de la Información

¿Existen procedimientos de mantenimiento de la Base de Datos y servidores? ¿Se encuentran por escrito?

¿Existen procedimientos para la recuperación de la Base de Datos? ¿Se encuentran por escrito?

¿Existen políticas y procedimientos para realizar los respaldos? ¿Se encuentran en forma escrita?

¿Los respaldos son almacenados dentro o fuera de la institución?

¿Se lleva un inventario de los respaldos realizados?

¿Se cuenta con políticas o procedimientos para asignar y autorizar el acceso de la información a los usuarios?

¿Se ha concientizado a los usuarios de los riesgos que puede originar el préstamo de sus contraseñas?

ENTREVISTA AL ADMINISTRADOR BASE DE DATOS

¿Cuál es la versión de Base de Datos?

¿Existen procedimientos de mantenimiento de la Base de Datos y servidores? ¿Se encuentran por escrito?

¿Existen procedimientos para realizar los respaldos? ¿Se encuentran por escrito?

¿Existen procedimientos para la recuperación de la Base de Datos? ¿Se encuentran por escrito?

¿Se someten a pruebas apropiadas los procedimientos de respaldo y de recuperación?

¿Se lleva por escrito un registro de las pruebas? Considerando:
Tiempo que toma recuperar
Proceso involucrado en la recuperación
Frecuencia de las pruebas
Fecha y resultados de la ultima prueba
Efectividad de las pruebas
Medidas posteriores adoptadas

¿El acceso al área de servidores es restringido?

¿Existe un control o bitácora de los ingresos al área de servidores?

¿El servidor se encuentra protegido a robo, incendio, alteraciones, cambio de voltaje? ¿Cuenta con ventilación suficiente?

¿El servidor cuenta con UPS?

¿Existe un estudio técnico reciente sobre la capacidad de dicha unidad?

¿Cuál es el nivel de respuesta que dan los proveedores de los servidores así como de los dispositivos que se encuentran en el área de servidores en caso de una eventualidad?

¿Se han adoptado medidas de seguridad (controles) para el acceso de la información?

¿Se tiene establecido qué información puede ser accesada y por cuáles personas?

¿El acceso a los archivos de datos y programas están restringidos por privilegios de sólo lectura, sólo consulta, lectura y escritura, crear, actualización, borrado, copiar?

¿Cuáles son las características de las contraseñas?

¿Cuándo el usuario es despedido o sale de vacaciones, se inactiva el usuario?

¿Las contraseñas se cambian frecuentemente?

¿La contraseña una vez que se define, es modificada por el usuario en el primer acceso que realiza?

¿Cuando la contraseña es cambiada, el sistema no permite que se vuelvan a utilizar contraseñas que ya fueron utilizadas?

¿Después de varias tentativas de acceso infructuosas, los usuarios son desconectados?

¿Se ha concientizado a los usuarios de los riesgos que puede originar el préstamo de sus contraseñas?

ENTREVISTA AL ENCARGADO SOPORTE TÉCNICO

¿Cuales son las características del equipo utilizado en el CTI?

¿Los computadores y el equipo de computo, están colocados más arriba del nivel del suelo?

¿Se utilizan reguladores de voltaje, para los computadores y fuente de poder especiales para los equipos grandes?

¿El equipo esta correctamente conectado a tierra como medida de protección contra rayos?

¿El acceso al área de servidores es restringido?

¿El servidor se encuentra protegido a robo, incendio, alteraciones, cambio de voltaje? ¿Cuenta con ventilación suficiente?

¿El servidor cuenta con UPS?

¿Existe un estudio técnico reciente sobre la capacidad de dicha unidad?

¿Se moviliza el equipo de servidores fuera del área destinada al mismo? ¿Con que fin?

¿Existen procedimientos para realizar los respaldos? ¿Se encuentran por escrito?

¿Los respaldos son almacenados dentro o fuera de la institución?

¿Se lleva un inventario de los respaldos realizados? ¿Qué datos contiene el inventario?

¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento?

¿Existen controles para el manejo de medios de almacenamiento masivo?

Controles físicos y ambientales empleados por la Institución así como los controles de acceso lógico.

La información que usted suministre será tratada de forma confidencial y sólo será utilizada para el presente estudio.

Se agradece su amable colaboración

¿Cuánto tiempo tiene de laborar en la Junta de Pensiones?
1 a 2 años _____ 3 a 4 años _____
5 a 6 años _____ 7 o más _____

¿Qué puesto desempeña actualmente? _____

¿Cuánto tiempo tiene de desempeñar el puesto?
1 a 2 años _____ 3 a 4 años _____
5 a 6 años _____ 7 o más _____

¿Cuándo usted ingresó a la institución recibió algún documento que le indicara el usuario y clave con las cuales podía hacer uso de los sistemas?

Si _____ No_____

¿Para hacer uso del computador cuenta usted con alguna contraseña, que lo identifique?

Si _____ No_____

¿Usted cuenta con la posibilidad de cambiar su contraseña en caso que lo necesite ?

Si _____ No_____

¿El sistema le solicita automáticamente el cambio de sus contraseñas en un tiempo determinado?

Si _____ No_____

¿Conoce algún documento emitido por la institución en el cual se especifique el uso de las contraseñas?

Si _____ No_____

En caso de tener algún problema con el sistema o el equipo. ¿Conoce el procedimiento que se debe seguir?

Si _____ No_____

Explique: _____
_____
_____

¿Puede reconocer si la causa del problema se debe a dificultades con el equipo o con los sistemas?

Si _____ No_____
Cite alguno:_____
_____
_____

¿Estos problemas son resueltos generalmente en:?
1 a 2 horas _____ 1 día _____ 1 semana _____
3 a 5 horas _____ 2 a 3 días _____ 2 a 3 semanas _____

¿ Ha recibido algún tipo de capacitación para el uso de los sistemas?
Si _____ No_____

¿ Ha recibido algún tipo de capacitación para el uso del equipo?
Si _____ No_____

¿En caso de falla de algún equipo informático, usted lo reporta inmediatamente a la División Informática?

Si _____ No_____

¿El equipo que utiliza cuenta con UPS?

Si _____ No_____

¿ El equipo que utiliza se encuentra ubicado más arriba del nivel suelo?

Si _____ No_____

¿Existen extintores en su área de trabajo?

Si _____ No_____

¿Conoce como utilizarlos ?

Si _____ No_____

¿En caso de ingresar a la División de Informática, el acceso es controlado por algún dispositivo de seguridad?

__ bitácora __ llavín eléctrico __ lector de carné __ ninguno

¿Tiene acceso al área de servidores?

Si _____ No_____

En caso de ser afirmativa

¿De que forma se controla el acceso?

__ bitácora __ llavín eléctrico __ lector de carné __ ninguno

Una vez que cuenta con acceso a los sistemas institucionales ¿tiene usted permiso de utilizar todas las opciones del sistema?

Si _____ No_____

¿Entre las opciones a las cuales tiene permiso, puede manipular completamente la información (agregar, modificar, borrar)?

Si _____ No_____

¿Tiene conocimiento de las políticas o disposiciones institucionales informáticas referente al uso del equipo y los sistemas?

Si _____ No_____

¿Existen compañeros que conozcan su identificación de usuario y contraseña de acceso tanto de los sistemas como del equipo?

Si _____ No_____

Cuando hace uso de cualquier medio de almacenamiento de origen externo a la institución, ¿usted revisa la existencia de virus?

Si _____ No_____

¿ Realiza respaldos frecuentemente de la información relevante y vital en su quehacer diario?

Si _____ No_____

¿Sabe que el equipo que se le ha asignado es de su responsabilidad y usted debe de mantenerlo en las mejores condiciones?

Si _____ No_____

¿Tiene conocimiento de los procedimientos a seguir en caso de una emergencia (Puede seleccionar más de una)?

Incendio _____ Terremoto_____
Inundación _____ Corte de Fluido eléctrico _____

¿Conoce las salidas de emergencia?

Si _____ No_____

¿Conoce la existencia de un comité de salud ocupacional en la institución?

Si _____ No_____

¿Pertenece usted al comité de salud ocupacional?

Si _____ No_____

En caso de NO pertenecer al comité ¿Conoce los integrantes del comité de salud ocupacional?

Si _____ No_____