UNIVERSIDAD MICHOACANA DE
SAN NICOLAS DE HIDALGO

FACULTAD DE CONTADURIA Y
CIENCIAS ADMINISTRATIVAS

PROPUESTA PARA LA CREACION DE LA COORDINACION DE INCIDENTES INFORMATICOS EN LA FCCA

T E S I S

PARA OBTENER EL TITULO DE:
LIC. EN INFORMATICA ADMINISTRATIVA

PRESENTA:
KARINA ISABEL TORRES PONCE

ASESOR:
M.A. SALVADOR ANTELMO CASANOVA VALENCIA

MORELIA, MICHOACAN, abril 2008

AGRADECIMIENTOS

A DIOS

En este espacio quiero agradecer a Dios, por que gracias a él he logrado cumplir mis metas que algún día fueron una simple idea, el me da la oportunidad de vivir y la sabiduría para saber hacerlo, estimula día a día con los detalles de la vida la razón de ser mejor, para mi, para mi familia y para todos los que me rodean. Dios Gracias esta Tesis es para ti.

A MAMA

Mi Mama ha sido el impulso que nunca me permitió mirar atrás, la energía para ser una persona dinámica, autentica y con valores. Esta tesis es el resultado de toda su fe, esfuerzo, trabajo y empeño que siempre puso en mí, esta Tesis es para ti MAMA por tu confianza y tú apoyo incondicional, Gracias.

A PAPA

Mi Papa que en paz descanse, siempre ha estado conmigo y gracias a él tengo ese intelecto tan despierto, que me ayuda a no tener miedo a ver y resolver las cosas con facilidad, para el nada era difícil o desconocido. Gracias PAPA esta Tesis es para ti.

A MI FAMILIA

Hermanos, Tíos, Abuelos, Gracias por estar siempre ahí como un pilar fuerte en el cual siempre me podía apoyar, mil Gracias.

A MI ESCUELA

Honorable, Universidad Michoacana de San Nicolás de Hidalgo, la máxima casa de estudios de Morelia Michoacán, Facultad de Contaduría Y Ciencias Administrativas, agradezco y dedico la presente Tesis.

A MIS PROFESORES

Agradezco, todo el conocimiento que me trasmitieron, así como su tiempo, compresión y tolerancia, mil Gracias.

A MÍ

Por que empezar una carrera, una tesis, es fácil, pero terminarla es realmente admirable. FELICIDADES KARINA logramos empezar el comienzo de una vida profesional muy interesante que todavía tiene mucho que descubrir.

GRACIAS A TODOS LO QUE FUERON PARTICIPES DE ESTE GRAN COMIENZO

INDICE

RESUMEN

Es importante ver que en las empresas o instituciones actualmente, es un verdadero problema la administración incorrecta de sus servicios informáticos y el erróneo manejo de los mismos, ocasionando pérdida de dinero, tiempo e información, esto producido por una mala administración en el equipo de cómputo. La información hoy en día es un activo muy importante para cualquier empresa o institución, motivo por el cual debe estar disponible para todos los niveles jerárquicos, para que en su momento puedan tomar una decisión correcta en base a la información obtenida, de no ser así esto afecta de forma notable a la empresa.

La presente tesis propone la creación de un centro único de primer contacto, dónde centralicen todos los incidentes informáticos que se presenten diariamente en la Facultad de Contaduría y Ciencias Administrativas, con la finalidad de tener un registro, control y ofrecer una solución a la brevedad posible del incidente. Con esta nueva disciplina se optimizan los recursos informáticos y se da fin al enorme despilfarro computacional que existe actualmente en la mayoría de las instituciones.

El objetivo principal es administrar correctamente todo el equipo de cómputo y sus recursos, obtener el control en situaciones donde ocurran fallas informáticas (bases de datos, Internet, redes, software, etc.) de nuestra institución, para lograr así la optimización de todo el equipo de cómputo, productividad en el trabajo por parte de los empleados y alumnos.

ABSTRACT

It is important to see that in the companies or institutions at the moment, it is a true problem the incorrect administration of their computer services and the erroneous handling of the same ones, causing loss of money, time and information, this taken place by a bad administration in the computation team. The information today in day is a very important asset for any company or institution, reason for which should be available for all the hierarchical levels, so that in its moment they can make a correct decision based on the obtained information, of not being this way this it affects from a remarkable way to the company.

The present thesis proposes the creation of an unique center of first contact, where all the computer incidents are centralized that is presented daily in the Ability of Accounting and Administrative Censes, this with the purpose of having a registration, control and to offer a solution to the possible brevity of incident. With this new discipline the computer resources are optimized and end is given to the enormous one I squander computational that exists at the moment in most of the institutions.

The main objective is to administer the whole computation team and its resources correctly, to obtain the control in situations where they happen computer flaws (databases, Internet, nets, software, etc.) of our institution, to achieve this way the optimization of the whole computation team, productivity in the work on the part of the employees and students.

INTRODUCCION

No hace mucho tiempo atrás todavía se ocupaban máquinas de escribir, calculadoras, enormes archiveros, carpetas entre un sin fin de herramientas de papelería para poder tratar de llevar un control y orden, sobre la operación administrativa que utilizaban en aquel tiempo la empresas o instituciones, pero los tiempos cambian y actualmente las computadoras y la informática es una necesidad para cualquier empresa, una necesidad que ayuda a tener información ordenada, y disponer de ella de forma rápida y eficaz.

Una computadora es una herramienta muy importante hoy en día, para cualquier tipo de empresa, la cual le da una ventaja competitiva para poder ahorrar tiempo en los procesos, reducir costos y desarrollar soluciones menos robustas para cubrir sus necesidades.

Este cambio radical implica diferentes formas de trabajar, y aunque ayuda a que la operación administrativa sea más rápida y eficiente, también tiene algunos desajustes que en ocasiones dificultan realizar el trabajo, pero para solucionar este tipo de eventos están los técnicos que son las personas indicadas para corregir cualquier anomalía en los equipos de cómputo.

En la actualidad las empresas cuentan con equipo de cómputo actualizado, que ayuda a aminorando el trabajo, pero aún así muchas empresas no han logrado administrar los recursos informáticos y esto ocasiona cierto descontrol, ya que si no administran correctamente los recursos informáticos esto ocasiona pérdidas en varios aspectos y entonces se convierte en una desventaja para la empresa.

Contar con computadoras para hacer más practica la operación de una empresa, implica también un costo, en cuanto al mantenimiento de los equipos, éste es un costo tanto material como humano por tal motivo; es necesario contar con personal capacitado para el uso de estos, y personal técnico para el mantenimiento de los equipos de cómputo.

Todo esto, nos recuerda las palabras de Ricardo Hernández Jiménez en su libro "Administración de la Función Informática AFI", él dijo:

"La informática en México ha sido invadida por la improvisación desmesurada, por eso jamás ha demostrado su verdadera entidad". Ricardo Hernández Jiménez.[1]

[1] Ricardo Hernández Jiménez, Administración de la Función. Informática, Editorial Trillas 2005

Generalmente las áreas de informática tienen problemas de operación en hardware, software, redes, etc. Esto inquieta y al mismo tiempo hace surgir las siguientes preguntas: ¿Cuáles son las razones?, ¿Qué es lo que pasa?, ¿Hay manera de eliminarlos o lo menos de abreviarlos? Es necesario hacer algo al respecto, pero antes es importante detectar los verdaderos problemas del ámbito informático y exponer las posibles soluciones.

¿Y para qué? En la actualidad la informática es una herramienta elemental en cualquier organización, empresa, oficina, trabajo, escuela, etc. Automatizar la información para hacer un trabajo más práctico, no es tarea fácil y en la actualidad las fallas informáticas afectan de manera notable y estas son muy costosas tanto en tiempo como en dinero, además desprestigian la labor del área de informática, ante sus propios usuarios fomentando constantes fricciones entre ambos.

"*Esta tecnología ha producido el fenómeno conocido como "despilfarro computacional" que consiste en la utilización errónea de los recursos informáticos, lo cual genera altos costos a mediano y largo plazo afectando la productividad y competitividad de una empresa".* Ricardo Hernández Jiménez.[2]

[2] Ricardo Hernández Jiménez, Administración de la Función. Informática, Editorial Trillas 2005

Existen algunas razones que entorpecen la función efectiva de la actividad informática, tales como:

* La mayoría de los jefes se comprometen a entregar resultados en tiempo record, sin tomar en cuenta quienes realmente hacen el trabajo.

* No existe una planeación efectiva, razón por la cual difícilmente realizan labor de investigación, necesaria para la mejor explotación de los recursos de cómputo.

* En gran cantidad de instalaciones el personal informático aprende sobre la marcha, de una manera completamente empírica y sin planes de capacitación plenamente establecidos.

* Las instalaciones no se encuentran acondicionadas de manera adecuada, esto origina riesgos el equipo de cómputo y esto impide que el recurso cubra el tiempo de vida correspondiente.

* El uso por parte de los usuarios no siempre es el adecuado, esto recorta el tiempo de vida útil de los equipos de cómputo.

* El acceso a usuarios no siempre esta restringido esto ocasiona que los sistemas sufran alteraciones lo que afecta la actividad diaria.

Como se puede apreciar, la problemática real está a la vista de todos y no en los recursos de cómputo como se pretende hacer creer, más bien se cree que *la raíz de todos estos desajustes es la falta de coordinación, motivación y disciplina*, factores indispensables en el ámbito informático.

En base a todo lo anterior, se ha pensado en una solución la cual servirá como herramienta para llevar un *registro, control y solución de todas las interrupciones* que se dan diariamente en el área de informática que existe en *la Facultad de Contaduría y C*iencias *Administrativas*, y de esta forma, implantar una nueva disciplina con la cual se logre una mejor productividad administrativa y un buen aprovechamiento sobre todo el recurso informático con el que cuenta la Institución.

Durante la operación diaria, los servicios de información suelen presentar eventos que reducen el nivel del servicio, este tipo de eventos los denominaremos *incidentes*.

Para minimizar el impacto que los incidentes ocasionan en las operaciones de los equipos de cómputo, se hace necesario establecer un procedimiento que tenga como objetivo reestablecer el servicio informático a la brevedad posible, así como tener un control minucioso y exhaustivo de las actividades relevantes diarias, nos referimos al procedimiento de *administración de incidentes*.

Para mantener una comunicación constante entre la operación administrativa que realiza diariamente la Facultad de Contaduría y Ciencias Administrativas, sobre el estado de los servicios informáticos, es necesario contar con un punto único de contacto denominado: **Coordinación de Incidentes Informáticos.**

En esta Coordinación se centralizarán diariamente todos los incidentes informáticos, para de esta forma llevar un control absoluto sobre todos y cada uno de ellos. Cada incidente será tratado y resuelto según la magnitud de este, ayudando así a que la interrupción del servicio informático tenga un bajo impacto.

Con la creación de **la Coordinación de Incidentes Informáticos en la F.C.C.A. ,** se canalizará cada uno de los incidentes que interrumpan el desarrollo de las operaciones diarias, con el fin de poder tener un control objetivo, veráz y concreto de los incidentes informáticos que ocurren constantemente en la administración de la Facultad de Contaduría y Ciencias Administrativas, y así poder resolverlos a la brevedad posible.

Registrar, controlar, solucionar y almacenar los reportes de incidentes, con el propósito de dar seguimiento a la atención de los mismos y analizar la información histórica para tomar acciones preventivas futuras, será una disciplina que ayudara a la Facultad de Contaduría y Ciencias Administrativas, a tener una operación constante y productiva.

La Coordinación de Incidentes Informáticos propuesta, tendrá al igual que cualquier otro departamento sus propios objetivos, normas y procedimientos, los cuales serán la razón de ser de esta. Tener un control de todos los incidentes Informáticos que ocurren en la Facultad de Contaduría y Ciencias Administrativas, para darles seguimiento buscando una pronta solución, para que la operación administrativa no pare sus labores por incidentes informáticos como hardware o software, es una de las principales objetivos que persigue la Coordinación de Incidentes Informáticos.

La forma en que funcionaría la Coordinación de Incidentes Informáticos sería de la siguiente manera: los usuarios se comunican por vía telefónica, correo electrónico o personalmente, para registrar las fallas técnicas informáticas que le impidan realizar sus actividades laborales cotidianas, de esta manera los analistas registraran el incidente y posteriormente darán seguimiento, para de esta forma dar una pronta solución a los diferentes tipos de incidentes que se registren, los niveles por los que tendrán que pasar los incidentes serán los siguientes.

Primer Nivel
Procedimiento de administración de incidentes
Segundo Nivel
Procedimiento de administración de la capacidad.
Tercer Nivel
Procedimiento de administración de problemas

La Coordinación de Incidentes Informáticos que se propone, esta orientado *al registro, control y solución* de *incidentes informáticos,* que ocurren día a día en la operación cotidiana de la Facultad de Contaduría y Ciencias Administrativas.

Esto con el fin claro de evitar que el personal que opera en dicha Facultad tenga que detener sus labores por un incidente o un minucioso detalle informático, llámese: Error de configuración, olvido de contraseña, instalación de un nuevo software, daño de alguna parte del hardware, errores de sistemas oficiales, etc.

Claro que no se pretenden evitar este tipo de anomalías, por que de cualquier forma son acciones que ocurren día a día por el simple hecho de utilizar algún servicio informático, pero lo que si se pretende evitar es, el descontrol de este tipo de situaciones y la pérdida de tiempo, por parte de los usuarios, por no conseguir una pronta solución a este tipo de situaciones.

Uno de los aspectos importantes que también analizaremos en este proyecto es determinar si será un gasto o una inversión crear a **la Coordinación de Incidentes Informáticos en la F.C.C.A.**

JUSTIFICACION

El equipo de cómputo en cualquier empresa representa un activo muy valioso, el cual se debe de cuidar y administrar al igual que cualquier otro recurso de la empresa, esto con el fin de no tener perdidas excesivas, el equipo de cómputo ayuda a la empresa a reducir costos, procesos y trabajo, pero si este no se administra correctamente puede que se convierta en un gasto en vez de una inversión para la empresa.

"El área de informática representa una entidad dentro de la organización, la cual tiene como objetivo satisfacer las necesidades de información de la empresa de manera veraz y oportuna. Su función primordial es complementar la labor administrativa para hacerla mas segura, fluida y así simplificarla. El área de informática es responsable entre muchas cosas más, de centralizar, custodiar y procesar la mayoría de los datos con los que opera la empresa. La toma de decisiones depende en gran medida de la capacidad de respuesta del proceso de datos. Por lo anterior, casi no se escatima la inversión para proveerla al área de informática del equipo técnico necesario (material y humano)." Ricardo Hernández Jiménez[3]

Con el fin de optimizar recursos, tiempos y costos es necesario implementar una administración de recursos informáticos, en la Facultad de Contaduría y Ciencias Administrativas, para apoyar esta determinación se propone crear **la Coordinación de Incidentes Informáticos en la F.C.C.A.**

[3] Ricardo Hernández Jiménez, Administración de la Función. Informática, Editorial Trillas 2005

La Coordinación de Incidentes Informáticos, será la responsable de concentrar toda la información relacionada con anomalías en los equipos de cómputo de la Facultad de Contaduría y Ciencias Administrativas, con lo cual se pretende tener un control y registro de todas las anomalías que sufran los equipos de cómputo, para así dar una solución a la brevedad posible.

Es necesario implementar esta nueva disciplina ya que es una forma de administrar, controlar y utilizar los recursos informáticos de la manera mas apropiada posible, de tal forma que a estos se les pueda obtener el mayor provecho posible y así optimizar todo el recurso informático con el que cuenta la Facultad.

La Coordinación de Incidentes Informáticos, es una necesidad que tiene que ser tomada en cuenta, ya que implantándose esta nueva administración sobre los recursos informáticos se esta hablando de obtener ventajas en cuanto al ahorro de recurso tanto económico como informático.

Sin duda alguna la implantación de la Coordinación de Incidentes Informáticos, es una muy buena propuesta para administrar todo el recurso informático que utiliza diariamente la Facultad de Contaduría y Ciencias Administrativas, y obtener así el mejor aprovechamiento de los recursos.

OBJETIVO GENERAL

Proponer la Creación de la Coordinación de Incidentes Informáticos en la F.C.C.A., la cual centralizará todas las fallas o anomalías que suceden diariamente con el servicio informático de la Facultad de Contaduría y Ciencias Administrativas, con la finalidad de administrar correctamente todo el equipo de cómputo y de esta forma optimizar y maximizar todo el recurso informático con el que cuenta dicha facultad y eliminar en un gran porcentaje el despilfarro computacional.

OBJETIVOS PARTICULARES

1. Atender todos los incidentes informáticos y que el usuario cuente con asesoría y asistencia técnica si es necesario, para que pueda continuar con sus labores, dar soluciones a los recursos informáticos para que estos sean una herramienta de trabajo y no un impedimento para concretarlo.

2. Administrar los recursos informáticos de la institución factor muy importe, para que esta tenga un control sobre las acciones que suceden cotidianamente, y de esta forma lograr que la operación administrativa u operativa, no sea interrumpida por tiempos prolongados.

Todas las instituciones y empresas buscan administrar correctamente todos sus recursos, actualmente son pocas las que logrado administrar sus recursos computacionales, inclusive hay quienes creen que no es necesario por tal motivo, esta tesis muestra la importancia de administrar correctamente los recursos computacionales y por que estos, tienen que estar disponibles en todo momento.

MARCO TEORICO

La Administración es una de las actividades humanas más importantes. Desde que los seres humanos comenzaron a formar grupos para alcanzar metas que no podían lograr individualmente, la Administración ha sido esencial para asegurar la coordinación de los esfuerzos individuales. A medida que la sociedad ha confiado cada vez más en el esfuerzo de grupo y que muchos grupos organizados se han vuelto grandes, las tareas de los administradores han cobrado cada vez más importancia.

La palabra "Administración", se forma del prefijo "ad", hacia, y de "ministrato". Esta última palabra viene a su vez de "ministre", vocablo compuesto de "minús.", Comparativo de inferioridad, y del sufijo "ter", que sirve como término de comparación. Si pues "magíster" (magistrado), indica una función de preeminencia o autoridad -el que ordena o dirige a otros en una función-, "ministre" expresa precisamente lo contrario: subordinación u obediencia; el que realiza una función bajo el mando de otro; el que presta un servicio a otro.

La etimología nos da pues de la Administración, la idea de que ésta se refiere a una función que se desarrolla bajo el mando de otro; de un servicio que se presta. Servicio y subordinación, son pues los elementos principales obtenidos.

La administración siempre esta enfocada a lograr fines o resultados.

DEFINICIÓN DE ADMINISTRACIÓN SEGÚN ALGUNOS AUTORES

Dentro de los principales pioneros de la administración, encontramos a los siguientes autores, los cuales definen a la administración como:

"Es la coordinación de todos los recursos a través del proceso de planeación, dirección y control, a fin de lograr los objetivos establecidos".

Henry Sisk Mario

"Es una ciencia social que persigue la satisfacción de objetivos institucionales por medio de una estructura y a través del esfuerzo coordinado".

José A. Fernández Arena

"Consiste en lograr un objetivo predeterminado mediante el esfuerzo ajeno".

George R. Ferry

"Así comprendida, la administración no es ni un privilegio exclusivo ni una carga personal del jefe o de los dirigentes de la empresa; es una función que se reparte, como las otras funciones esenciales, entre la cabeza y los miembros del cuerpo social."

Mary P. Follett

(Considerado por muchos como el verdadero padre de la Administración moderna), dice que "administrar es prever, organizar, mandar, coordinar y controlar".

Henry Fayol

"Es un conjunto sistemático de reglas para lograr la máxima eficiencia en las formas de estructurar y manejar un organismo.

A. Reyes Ponce

“Administración es la acción y efecto de administrar, es la aplicación de una cosa a un fin. A su vez administrar es gobernar, regir, manejar, cuidar los negocios o intereses, públicos o privados, propios o ajenos.”

“Proceso de crear, diseñar y mantener un ambiente en el que las personas al laborar o trabajar en grupos, alcancen con eficiencia metas seleccionadas.
Las personas realizan funciones administrativas de planeación, organización, integración de personal, dirección y control.”

Esta se aplica a todo tipo de organizaciones bien sean pequeñas o grandes empresas lucrativas y no lucrativas, a las industrias manufactureras y a las de servicio.

Según el diccionario académico de la lengua española.

IMPORTANCIA DE LA ADMINISTRACIÓN

La administración es un órgano social específicamente encargado de hacer que los recursos sean productivos, refleja el espíritu esencial de la era moderna, es indispensable y esto explica por que una vez creada creció con tanta rapidez y tan poca oposición.

La administración busca el logro de objetivos a través de las personas, mediante técnicas dentro de una organización. Ella es el subsistema clave dentro de un sistema organizacional. Comprende a toda organización y es fuerza vital que enlaza todos los demás subsistemas.

Proceso Administrativo

El proceso administrativo se define como el proceso metodológico que implica una serie de actividades que llevará a una mejor consecución de los objetivos, en un periodo más corto y con una mayor productividad.

El proceso administrativo se dice que es tridimensional, porque sus elementos son aplicables a todas las funciones del organismo en todos sus niveles:

- Planeación.
- Organización.
- Dirección y control.

El proceso administrativo se da en varias etapas según los autores que a continuación se les presentan:

Henry Fayol. Etapas: Previsión, organización, comando, coordinación y control.

G. R. Terry. Etapas: Planeación, organización, dirección y control.

Agustín Reyes Ponce. Etapas: Previsión, planeación, organización, integración, dirección y control.

G. R. Ferry: Planeación, Organización, Dirección, Control.

A lo largo de la humanidad, el hombre ha creado ciencias que le permiten conocer y estudiar fenómenos acontecidos, esta curiosidad lo llevo a crear las computadoras u ordenadores, y a partir de ellos surge la implementación de la informática.

En sus inicios, la informática facilitó los trabajos repetitivos y monótonos del área administrativa, gracias a la automatización de esos procesos, lo que a su vez trajo como ventaja una disminución de los costes.

A lo largo de la historia de la informática, se ha demostrado su utilidad en el manejo de información rápida, precisa y fiable. Dentro del concepto de informática, su principal función es facilitar información oportuna y veraz, lo cual facilita la toma de decisiones a nivel empresarial.

El vocablo Informática proveniente del francés *informatique*, acuñado por el ingeniero Philippe Dreyfus en 1962, acrónimo de las palabras *information* y *automatique*.

Entonces, el concepto de informática viene dado de la unión de dos palabras **Infor**macion y auto**mática**.

Hoy también se le conoce como manejo de sistemas de información, procesamiento de datos o ciencia de la computación.

DEFINICIÓN DE INFORMATICA SEGÚN ALGUNOS AUTORES

"Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores".

Según el diccionario académico de la lengua española.

"La informática es la ciencia que se encarga del tratamiento automático de la información. Este tratamiento automático es el que ha propiciado y facilitado la manipulación de grandes volúmenes de datos y la ejecución rápida de cálculos complejos".

José Miguel Blázquez

La informática es la disciplina que estudia el tratamiento automático de la información utilizando dispositivos electrónicos y sistemas computacionales. También es definida como el procesamiento de información en forma automática. Para ello los sistemas informáticos deben realizar las siguientes tareas básicas:

Entrada: Captación de información.
Procesamiento o tratamiento de dicha información.
Salida: Transmisión de resultados.

Podemos entender el concepto de informática como aquella ciencia encargada de estudiar los ordenadores y su capacidad para procesar y almacenar información y datos.

La informática es aplicada en diversos sectores de la actividad diaria tales como: La medicina, ingeniería, industria, en la investigación científica, el arte y a nivel empresarial. También se utiliza en la elaboración de documentos, monitorización y control de procesos, robots industriales, telecomunicaciones, desarrollo de juegos, aplicaciones/herramientas multimedia, etc.

Las funciones principales de la informática son las siguientes:

Creación de nuevas computadoras.

Creación de nuevas especificaciones de trabajo.

Desarrollo e implementación de sistemas informáticos.

Optimización de los métodos y sistemas informáticos existentes.

En la informática convergen los fundamentos de las ciencias de la computación (hardware), la programación y las metodologías para el desarrollo de software, la arquitectura de computadoras, las redes de datos como Internet, la inteligencia artificial, así como determinados temas de electrónica. Se puede entender por *informática* a la unión de todo este conjunto de disciplinas.

La Administración Informática, utiliza los procedimientos más eficientes y productivos utilizando las nuevas tecnologías, estudia los procesos correctos que debe tener la información a través de los medios computacionales, para la toma de decisiones en un mundo informático cambiante.

La administración tiene una relación muy importante respecto a la informática, ya que la informática también requiere ser administrada, para que los recursos informáticos coordinados con la administración logren obtener los resultados esperados.

La administración informática es la forma en que se administra todo el recurso informático, utilizándolo de manera eficiente y eficaz y de esta manera optimizar este recurso obteniendo así el mejor provecho de este.

La informática dentro de una empresa tiene un papel muy importante ya que tiene una relación muy estrecha con todos los departamentos pues en base a la informática, estos operan constantemente y por dicha razón están relacionados.

El área de Informática en las organizaciones, tiene contacto con Recursos Humanos, Presupuestos, Adquisición de Recursos Computacionales y con los usuarios Finales y sus necesidades.

Dado que la informática esta en todos los departamentos y es un recurso muy importante dentro de la organizaciones este no debe pasar desapercibido, en cuanto a llevar una correcta y exhaustiva administración respecto a ella.

Actualmente toda empresa o institución, cuenta por lo menos con una computadora para llevar la administración de esta, esto es una necesidad que ya no se puede dejar atrás apoyarse de la tecnología para lograr llevar un control mas optimizado en su administración tanto de procesos como de oficina es una necesidad constante que tiene las empresas hoy en día, razón por la cual la informática esta muy ligada a la administración ya que sin esta sería complicado lograr tener una mas práctica y correcta administración.

La informática y la administración son ciencias muy importantes actualmente, para cualquier empresa o rubro social, ya que en base a esta se toman decisiones de cualquier índole, si todas las empresa automatizan toda su información y administrar todos sus recursos, estas indudablemente lograran obtener el éxito esperado.

Un Centro de cómputo, es el conjunto de recursos físico, lógicos, y humanos necesarios para la organización, realización y control de las actividades informáticas de una empresa o institución.

Las principales funciones que se requieren para operar un centro de cómputo son las siguientes:

- Operar el sistema de computación central y mantener el sistema disponible para los usuarios.
- Ejecutar los procesos asignados conforme a los programas de producción y calendarios preestablecidos, dejando el registro correspondiente en las solicitudes de proceso.
- Revisar los resultados de los procesos e incorporar acciones correctivas conforme a instrucciones de su superior inmediato.
- Realizar las copias de respaldo (back-up) de la información y procesos de cómputo que se realizan en la Dirección, conforme a parámetros preestablecidos.
- Marcar y/o señalizar los productos de los procesos ejecutados.
- Llevar registros de fallas, problemas, soluciones, acciones desarrolladas, respaldos, recuperaciones y trabajos realizados.
- Velar porque el sistema computarizado se mantenga funcionando apropiadamente y estar vigilante para detectar y corregir fallas en el mismo.
- Realizar labores de mantenimiento y limpieza de los equipos del centro de cómputo.
- Aplicar en forma estricta las normas de seguridad y control establecidas.
- Mantener informado al jefe inmediato sobre el funcionamiento del centro de cómputo.
- Cumplir con las normas, reglamentos y procedimientos establecidos por la Dirección para el desarrollo de las funciones asignadas.

El principal objetivo de un centro de cómputo es el de concentrar el procesamiento de datos e información de una manera sistematizada y automática.

La computadora como herramienta de solución para problemas de cálculo de operaciones, investigación de procesos, enseñanza, etc. establece las bases para determinar el objetivo de un centro de cómputo, como es el de prestar servicios a diferentes áreas de una organización ya sea dentro de la misma empresa, o bien fuera de ella, tales como: producción, control de operaciones, captura de datos, programación, dibujo, biblioteca, etc. Los diversos servicios que puede prestar un centro de cómputo, pueden dividirse en departamentos a áreas específicas de trabajo.

Algunos puestos que operan en un centro de cómputo son:

- Analistas
- Gerente de proceso.
- Programador de sistemas.
- Supervisor de capturistas.
- Capturistas.
- Dibujante.
- Soporte técnico.

A su vez un centro de cómputo cuenta con división de departamento tales como:

- Soporte técnico a usuarios
- Gestión y administración del propio Centro de Procesamiento de Datos
- Departamento o área de Operación.
- Departamento o área de Producción y Control
- Departamento o área de Análisis de Sistemas
- Departamento o área de Programación.
- Departamento o área de Implementación.
- Departamento o área de Soporte Técnico.

1. COORDINACION DE INCIDENTES INFORMATICOS

Área en la cual se centralizan todos los incidentes informáticos de la Facultad de Contaduría y Ciencias Administrativas, se les da solución a diferentes niveles según sea el caso, esta área cuenta con personal capacitado, para dar el servicio de ayuda a los usuarios en fases como asesoría o asistencia técnica, siempre que estos lo soliciten.

La Coordinación de Incidentes Informáticos, es la encargada de registrar, almacenar y solucionar todos los incidentes informáticos diarios, logrando tener un control absoluto sobre todos los eventos que interrumpan el servicio informático dentro de la Facultad de Contaduría y Ciencias Administrativas, para poder tomar medidas preventivas, y obtener el mayor rendimiento y aprovechamiento sobre los servicios informáticos, también es la responsable de **administrar correctamente** todo el recurso computacional así como la protección de los laboratorios y de todo el equipo de de computo con el que cuenta dicha facultad.

PROPUESTA

La presente tesis propone, crear un centro de primer contacto donde se lleve un registro, control y solución de todos los incidentes informáticos de la Facultad de Contaduría Ciencias Administrativas, para lograr administrar correctamente todo el recurso informático con el que cuenta esta.

El área donde se centralizaran todos los incidentes informáticos se le denominara: **Coordinación de Incidentes Informáticos;** en este lugar todos los usuarios contaran con ayuda para resolver sus incidencias cotidianas en lo que corresponde al servicio informático, aquí se dispondrá de gente capacitada para resolver todas las anomalías trátese de hardware, software, redes, internet, impresoras, etc.

El presente proyecto fortalecerá el área informática de toda la facultad, ya que las interrupciones del servicio informático se reducirían de manera notable, y se comenzaran a administrar los recursos informáticos de manera en que estos optimicen su tiempo de vida útil, y ofrezcan al usuario el servicio correspondiente en el momento que este lo requiera.

OBJETIVOS GENERALES Y PARTICULARES DE COORDINACION DE INCIDENTES INFORMATICOS

OBJETIVO GENERAL

Disponer de un punto único donde se canalicen todos los incidentes informáticos, con la finalidad de tener un control exhaustivo de este tipo de eventos, evitando el constante despilfarro computacional y aprovechar los recursos informáticos de forma adecuada.

OBJETIVOS PARTICULARES

- Registrar incidentes informáticos, para que ayude a minimizar perdidas de recursos informáticos.
- Solucionar a la brevedad posible para que los equipos de cómputo de verdad faciliten el trabajo diario.
- Disminuir de manera notable la interrupción de los servicios informáticos.
- Disminuir de manera notable las pérdidas, o bien el despilfarro informático.
- Dar el mantenimiento oportuno a todos los equipos de cómputo de la Facultad de Contaduría y Ciencias Administrativas para optimizar el tiempo de vida útil de estos.
- Controlar y darle seguimiento de manera oportuna a los incidentes informáticos que ocurren constantemente.
- Crear una nueva disciplina para todos los usuarios que operan en los equipos de cómputo de la Facultad de Contaduría y Ciencias Administrativas, para optimizar recursos de manera notable.
- Documentar soluciones de primer nivel para que estén al alcance de todos.
- Administrar correctamente los recursos informáticos.

MISIÓN

Nuestra misión es, registrar, controlar y solucionar toda clase de incidentes informáticos, así como administrar correctamente los recursos computaciones de la Facultad de Contaduría y Ciencias Administrativas, minimizar el impacto de incidentes y reestablecer el servicio a la brevedad posible, brindar a todos los usuarios un servicio de calidad para que no interrumpan sus actividades laborales o escolares cotidianas, y de esta forma puedan disponer de los servicios informáticos de una manera adecuada y productiva.

VISIÓN

Lograr tener una administración correcta de todo el recurso informático para optimizar el uso, de los recursos computacionales, eliminando el despilfarro informático de la Facultad de Contaduría Ciencias Administrativas.

ALCANCE

La Coordinación de Incidentes Informáticos, esta dirigida a todos los usuarios de servicios informáticos de la Facultad de Contaduría y Ciencias Administrativas, pueden ser alumnos de laboratorios de cómputo, personal administrativo y docente académico.

En caso de que se presente algún incidente informático los usuarios tendrán que comunicarse vía telefónica, enviar un correo electrónico o bien levantar su reporte personalmente, a **la Coordinación de Incidentes Informáticos.**

1.1 ¿QUE ES LA COORDINACION DE INCIDENTES INFORMATICOS EN LA F.C.C.A.?

El principal objetivo de un centro de cómputo es el de concentrar el procesamiento de datos e información de una manera sistematizada y automática.

La *coordinación* es un proceso que consiste en integrar las actividades de departamentos independientes a efectos de perseguir las metas de la organización con eficacia. Sin coordinación, la gente perdería de vista sus papeles dentro de la organización y enfrentaría la tentación de perseguir los intereses de su departamento, a expensas de las metas de la organización.

La Coordinación de Incidentes Informáticos, es el área responsable de llevar e*l registro, control y solución* de *incidentes informáticos,* que ocurren día a día en la operación cotidiana de, la Facultad de Contaduría y Ciencias Administrativas.

Esto con el fin, de evitar que el personal que opera en dicha Institución no tenga que detener sus labores por un incidente o un minucioso detalle informático, por ejemplo:

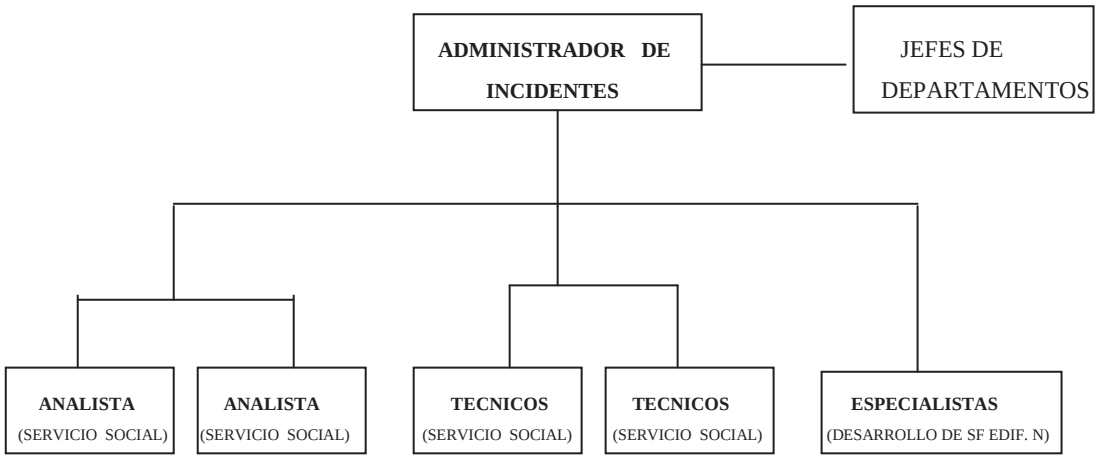
* Error de configuración
* Olvido de contraseña
* Instalación de un nuevo software
* Daño de alguna parte del hardware
* Errores de sistemas oficiales.
* Fallas con la red.
* Fallas con el internet.
* Problemas con impresoras.

La Coordinación de Incidentes Informáticos, es una nueva forma de trabajar, la cual esta orientada única y exclusivamente a resolver y administrar todos los incidentes informáticos a la brevedad posible, para evitar un fuerte impacto en la operación de los servicios informáticos, que se lleva diariamente en la Facultad de Contaduría Ciencias Administrativas.

La Coordinación de Incidentes Informáticos, se consolida como un centro de cómputo con las mismas características tanto de software, hardware y seguridad que suelen tener, lógicamente de acuerdo a las necesidades de este. Es un centro de cómputo que también persigue cierta meta, la cual es tener la información veraz sobre los incidentes informáticos, su procedimiento respectivo y tener un control absoluto sobre los recursos informáticos de la Facultad de Contaduría y Ciencias Administrativas.

No es un departamento solamente, esta considerado como una Coordinación que en este caso será la responsable de coordinar los departamentos de la Facultad de Contaduría y Ciencias Administrativas, en cuanto a las interrupciones informáticas que sufren estos, mediante su operación cotidiana y les apoya a reestablecer el servicio.

ORGANIGRAMA PROPUESTO PARA LA COORDINACION DE INCIDENTES INFORMATICOS:



1.2 ¿CÓMO FUNCIONARIA LA COORDINACION DE INCIDENTES INFORMATICOS EN LA F.C.C.A?

La Coordinación de Incidentes Informáticos, es un departamento donde el personal se encarga de recibir llamadas, correos y reportes que levanten personalmente los usuarios para posteriormente dar de alta el incidente, si está dentro de las posibilidades del analista la solución lleva a cabo la pronta solución del incidente, si no es así el incidente es escalado a un segundo nivel.

Los usuarios una vez que se presenta cualquier tipo de incidente ante ellos, se comunican a **la Coordinación de Incidentes Informáticos**, vía telefónica, correo electrónico o personalmente, levantan el reporte sobre el incidente informático que le impida realizar sus actividades laborales cotidianas, de esta manera los analistas registraran el incidente y posteriormente darán seguimiento a este ya sea vía telefónica, o bien enviando a un especialista en determinado aspecto que se halla reportado, para de esta forma dar una pronta solución a los diferentes tipos de incidentes que se registren.

Se piensa con este proyecto tener un control automatizado de todas las fallas que existan en la Facultad de Contaduría y Ciencias Administrativas, con el fin de tener un registro de todas y cada una de ellas y así saber cuando ocurrió, en que máquina, quien la opera, si se dio pronta solución, si no fue así por qué fue, y con esto evitar que el personal pare sus actividades por incidentes informáticos.

Existen niveles por los que tendrán que pasar cada uno de los incidentes según el caso de cada uno de ellos.

Primer Nivel

Analistas

Procedimiento de administración de incidentes

Aquí se identifica al usuario, de donde llama, datos personales de empleado o estudiante, posteriormente con que elementos esta conectado o tiene relación y si los elementos en uso están autorizados, una vez analizado esto, se apoyara en la gestión de la manera correspondiente para que a este nivel se pueda resolver el incidente del usuario de lo contrario que escale a segundo nivel.

Segundo Nivel

Especialistas

Procedimiento de administración de la capacidad.

Una vez analizado el incidente que acaba de reportar el usuario, si no fue resuelto en el primer nivel pasa al segundo nivel donde se canaliza con un especialista en el área el cual cuenta con la capacidad para resolverlo, trátese de software, hardware o instalación de los equipos. Si aun siendo así existe la posibilidad de que por algún motivo, razón o circunstancia no se de una solución, motivo por el cual tendrá que ser escalado a tercer nivel.

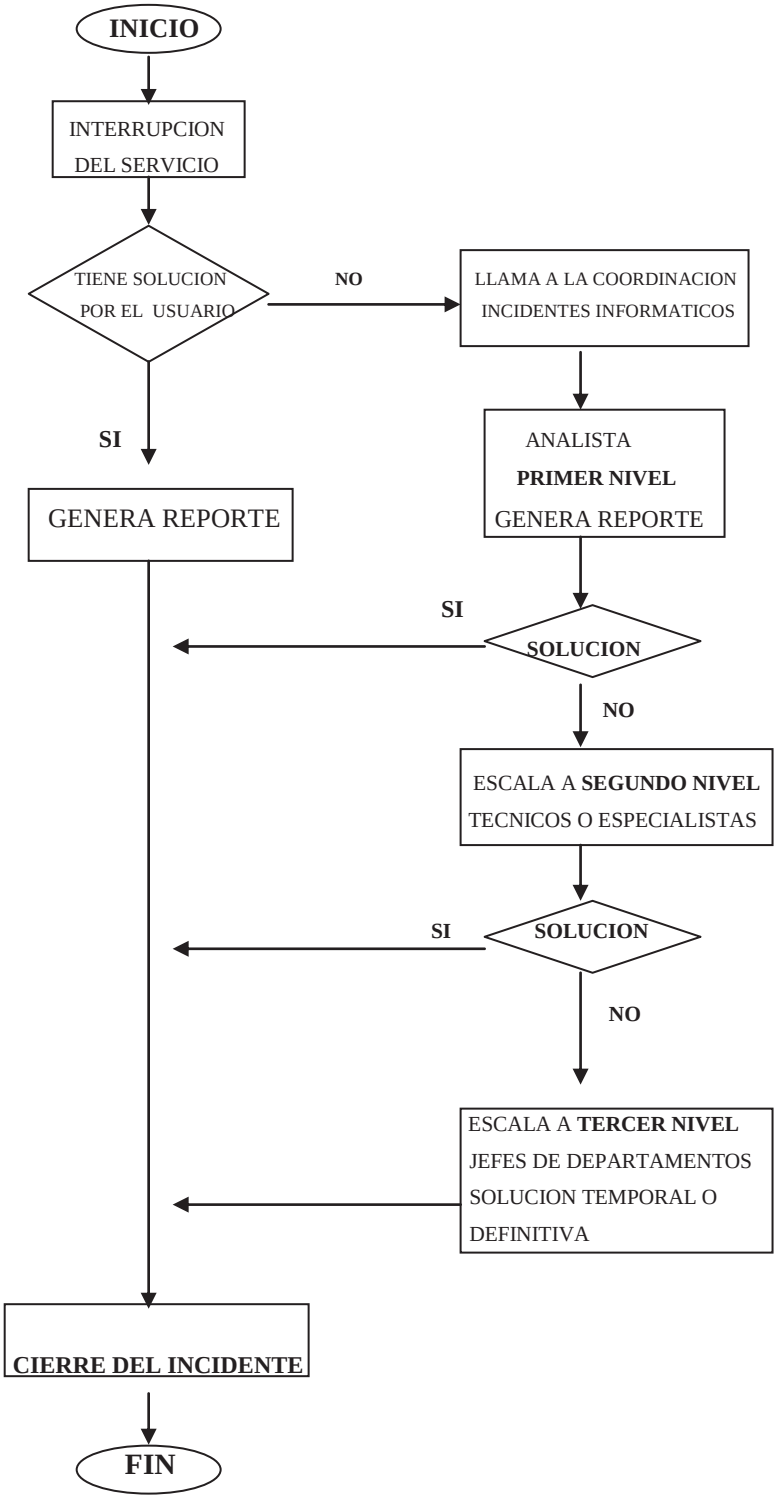
Tercer Nivel

Jefes toma de decisiones

Procedimiento de administración de problemas

Cuando el incidente en primer nivel se analizó y no tuvo una pronta respuesta satisfactoria, pasa con el especialista a segundo nivel y si persiste de igual forma sin ser resuelto, pasa a convertirse de incidente a problema y alcanza su último nivel de escalamiento, una vez atendido por el *"Procedimiento de Administración de Problemas"* este regresa ya con una solución definitiva.

Enseguida se muestra un esquema sobre la serie de pasos por la que pasa cada incidente



1.3 ANALISIS DE LA DEMANDA DEL SERVICIO

La Facultad de Contaduría y Ciencias Administrativas, cuenta con cuatro edificios el **Y, Z, A-II, y A-IV**, estos ubicados dentro del campus de la Universidad Michoacana de San Nicolás de Hidalgo.

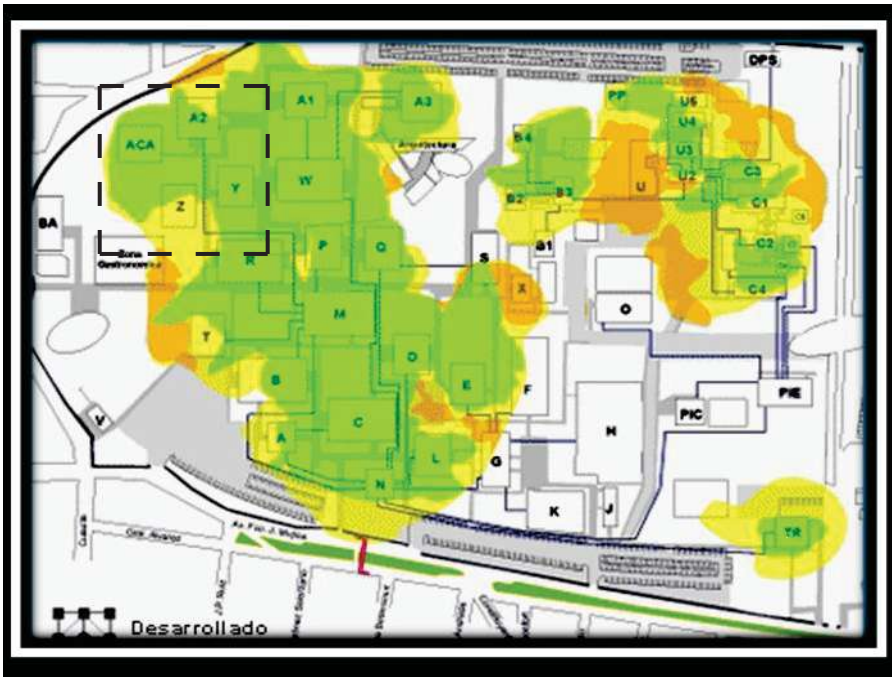
Edificios en los que actualmente se imparten tres diferentes Licenciaturas;

Lic. En Administración

Lic. En Contaduría

Lic. En Informática Administrativa

El siguiente mapa muestra donde se encuentran ubicados los edificios de La Facultad de Contaduría y Ciencias **Administrativas.**



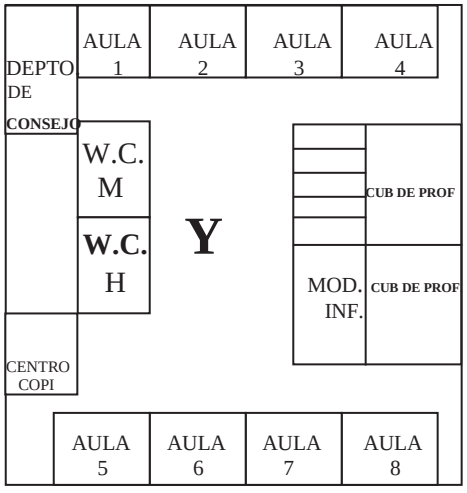
A continuación se realizara un inventario en cada uno de los edificios, para corroborar la ubicación física de las computadoras con las que cuenta la Facultad de Contaduría y Ciencias Administrativas.

FACULTAD DE CONTADURIA Y CIENCIAS ADMINISTRATIVAS
EDIFICIO Y

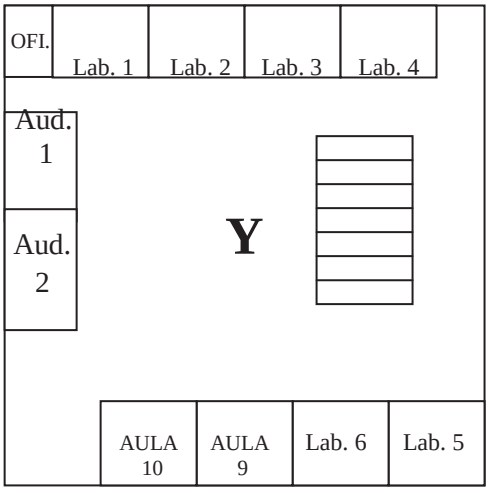
PLANTA BAJA
Aulas De La F.C.C.A.
Modulo De Información. F.C.C.A
Departamento De Consejo Técnico
Cubículos De Profesores
Área De Fotocopiado

PLANTA ALTA
Laboratorios De Computo F.C.C.A.
Salas Audiovisuales
Oficina

PLANTA BAJA



PLANTA ALTA



EL EDIFICIO Y CUENTA CON EL SIGUIENTE EQUIPO DE CÓMPUTO:

PLANTA BAJA
Aulas De La F.C.C.A.
Coordinación de Asistencia. F.C.C.A.
Departamento de consejo técnico.
Coord. De Capacitación**.**
Área De Fotocopiado.

PLANTA ALTA
Laboratorios De Computo.
Salas Audiovisuales.
Oficina de informática.

Entonces, se tiene que en el edifico **Y** se cuenta con 168 computadoras funcionando.

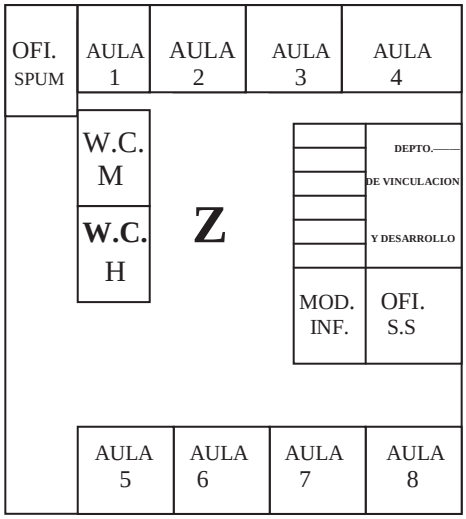
N de deptos.	DEPARTAMENTO		N. De Pc´s		Total
6	Laboratorios de Cómputo	*	27 Pc´s	=	162
1	Consejo Técnico	*	1 Pc	=	1
1	Coord. De Asistencia	*	3 Pc	=	3
1	Coord. De Capacitación	*	1 Pc	=	1
1	Oficina de Informática	*	1 Pc	=	1
TOTAL					**168 Pc´s**

FACULTAD DE CONTADURIA Y CIENCIAS ADMINISTRATIVAS
EDIFICIO Z

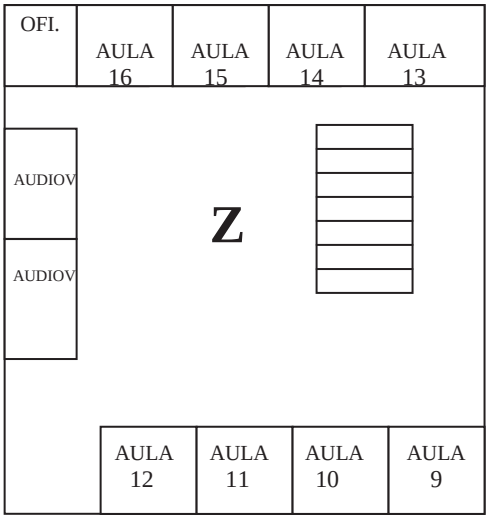
PLANTA BAJA
Aulas De La F.C.C.A.
Cubículos De La Sección Sindical (Spum).
Coordinación Del Servicio Social.
Departamento De Vinculación Y Desarrollo
Modulo De Información F.C.C.A.

PLANTA ALTA
Aulas De La F.C.C.A.
Salas Audiovisuales

PLANTA BAJA



PLANTA ALTA



EL EDIFICIO Z CUENTA CON EL SIGUIENTE EQUIPO DE CÓMPUTO

PLANTA BAJA
Aulas De La F.C.C.A.
Cubículos De La Sección Sindical.
Coordinación Del Servicio Social.
Departamento De Vinculación Y Desarrollo.
Modulo De Información F.C.C.A.
Coordinación de Egresados.

PLANTA ALTA
Aulas De La F.C.C.A.
.

Entonces, se tiene que en el edifico **Z** se cuenta con 7 computadoras funcionando.

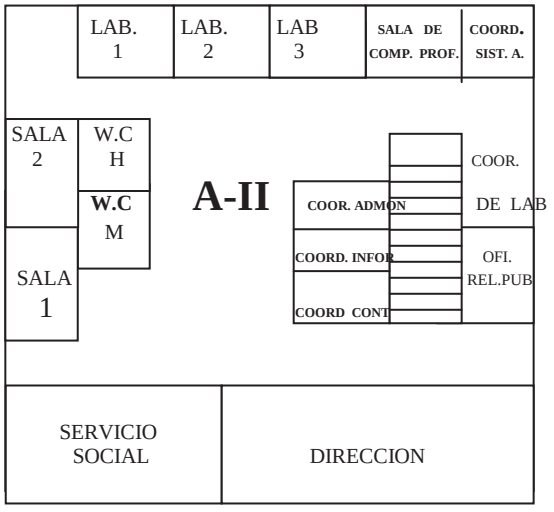
N de deptos.	DEPARTAMENTO		N. De Pc´s		Total
1	Cubículo Sindical	*	2 Pc	=	2
1	Coord. Del Serv. Soc.	*	2 Pc	=	2
1	Depto De Vinc Y Des	*	1 Pc	=	1
1	Mod De Inf.	*	1 Pc	=	1
1	Coord de Egresados	*	1 Pc	=	1
Total					**7 Pc´s**

FACULTAD DE CONTADURIA CIENCIAS ADMINISTRATIVAS
EDIFICIO A-II

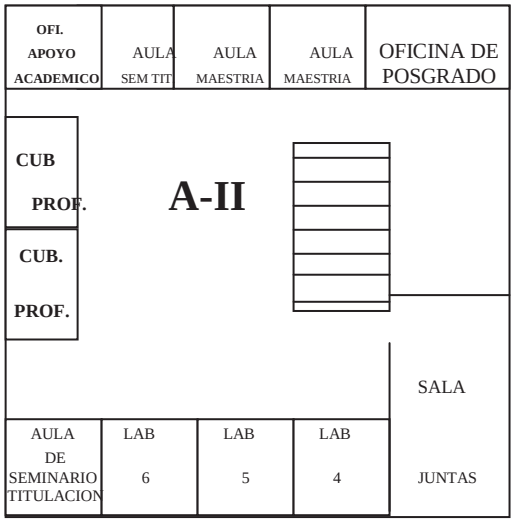
PLANTA BAJA
Oficinas De La Dirección F.C.C.A.
Oficinas De Control Escolar F.C.C.A..
Salas De Exámenes Recepcionales F.C.C.A.
Laboratorios De Computo F.C.C.A.
Sala De Computo Para Profesores F.C.C.A.
Coordinaciones Administración, Contaduría e Informática F.C.C.A.
Coordinación del sistema abierto.
Oficina De Relaciones Públicas F.C.C.A.
Coordinación de laboratorios F.C.C.A.

PLANTA ALTA
Oficina Del Postgrado F.C.C.A.
Aulas Para Maestrías En Administración F.C.C.A
Aulas Para Seminarios De Titilación F.C.C.A.
Sala De Juntas.
Oficina De Apoyo Académico
Laboratorios De Computo F.C.C.A
Cubículos De Profesores F.C.C.A

PLANTA BAJA



PLANTA ALTA



EL EDIFICIO A-II CUENTA CON EL SIGUIENTE EQUIPO DE CÓMPUTO.

PLANTA BAJA

Oficinas De La Dirección De La F.C.C.A.
Oficinas De Control Escolar De La F.C.C.A.
Laboratorios De Computo F.C.C.A
Sala De Computo Para Profesores De La F.C.C.A.
Coordinaciones Admón., Cont. e Infor. F.C.C.A.
Coordinación del sistema abierto.
Salas De Exámenes Recepcionales F.C.C.A.
Coordinación de laboratorios F.C.C.A.

PLANTA ALTA

Oficina Del Postgrado De La F.C.C.A.
Aulas Para Maestrías En Administración F.C.C.A
Aulas Para Seminarios De Titilación F.C.C.A.
Sala De Juntas.
Oficina De Apoyo Académico.
Laboratorios De Computo F.C.C.A.
Cubículos De Profesores F.C.C.A.

Entonces, se tiene que en el edifico **A-II,** se cuenta con 208 computadoras funcionando.

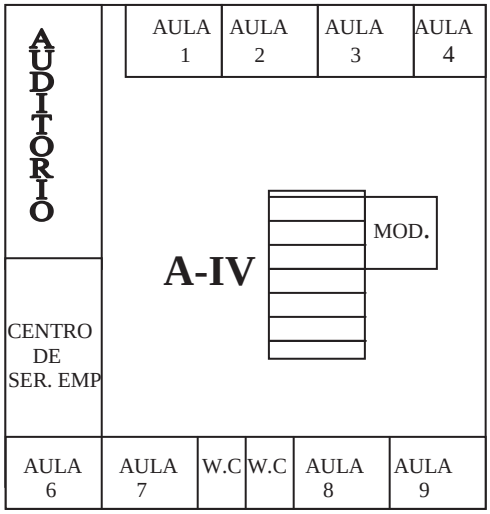
N de deptos.	DEPARTAMENTO		N. De Pc´s		Total
1	Dirección F.C.C.A.	*	8 Pc´s	=	8
1	Control Escolar F.C.C.A.	*	7 Pc´s	=	7
6	Laboratorios de Computo	*	24 Pc´s	=	145
1	Laboratorio de Computo de Profesores	*	10 Pc´s	=	10
5	Coord. Admon., Cont., Iinfor., Sist abie.	*	1 Pc´s	=	5
1	Coordinación de Informática	*	14 Pc´s	=	14
2	Aulas de Maestría	*	3 Pc	=	6
	Cubículos de Profesores	*	13 Pc´s	=	13
	Total			=	**208**

FACULTAD DE CONTADURIA Y CIENCIAS ADMINISTRATIVAS
EDIFICIO A-IV

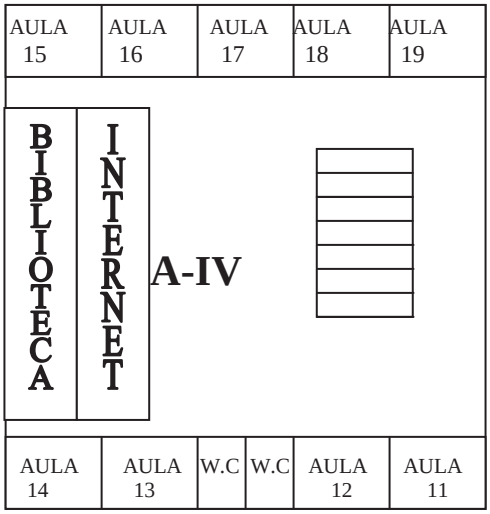
PLANTA BAJA
Aulas De La Facultad De Contaduría Y Ciencias Administrativas
Auditorio F.C.C.A.
Centro De Servicios Empresariales
Modulo De Información F.C.C.A

PRIMER NIVEL
Aulas De La Facultad De Contaduría Y Ciencias Administrativas
Biblioteca
Internet

PLANTA BAJA

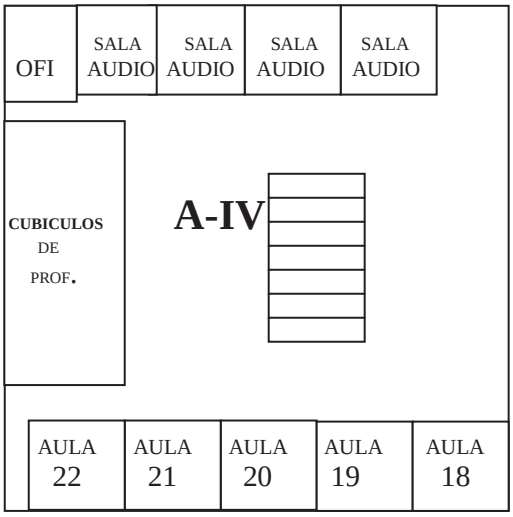


PRIMER NIVEL



SEGUNDO NIVEL
Aulas De La Facultad De Contaduría Y Ciencias Administrativas
Salas Audiovisuales
Cubículos De Profesores
Oficina

SEGUNDO NIVEL



EL EDIFICIO A- IV CUENTA CON EL SIGUIENTE EQUIPO DE CÓMPUTO.

PLANTA BAJA
Aulas De La F.C.C.A.
Auditorio F.C.C.A.
Centro De Servicios Empresariales.
Coordinación de Asistencia.

PRIMER NIVEL
Aulas De La F.C.C.A.
Biblioteca.
Centro de Internet .

SEGUNDO NIVEL
Aulas De La F.C.C.A
Salas Audiovisuales.
Cubículos De Profesores.
Coordinación del deporte.

Entonces, se tiene que en el edifico **A- IV,** se cuenta con 23 computadoras funcionando.

N de deptos.	DEPARTAMENTO		N. De Pc´s		Total
1	Coordinación de Asistencia	*	1	=	1
1	Centro de Servicios Empresariales	*	3	=	3
1	Biblioteca	*	4	=	4
1	Centro de Internet	*	14	=	14
5	Coord. Del Deporte	*	1	=	1
Total					**23**

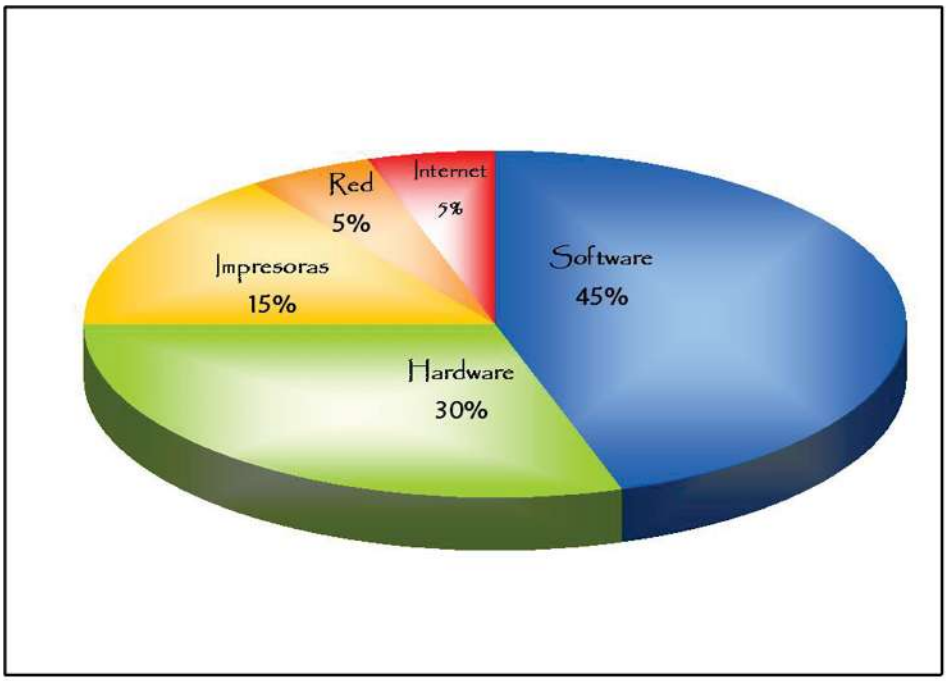
En la Faculta de Contaduría y Ciencias Administrativas se cuenta con un promedio de 536 unidades en equipo de computo (anexo 1, inventario detallado de las unidades), tomando en cuenta los cuatro edificios con los que cuenta dicha facultad.

EDIFICIO	**N. DE PC´S**
Y	168
Z	7
A-II	208
A- IV	23
Laptos	16
Impresoras	42
Bocinas	40
Cañones	21
Pantallas	7
Scaner	4
TOTAL	**536**

Como se puede apreciar es un numero significativo y mas aún, si estamos hablando de equipo de cómputo, que esta en constante operación y que sufre diariamente diferentes tipos de incidencias, las cuales hasta el día de hoy no existe un procedimiento concreto, por medio del cual se les de solución a cada una de estas computadoras en caso de requerirlo, motivo por el cual los tiempos de respuesta son prolongados, cuando hay problemas con el servicio informático, esto retrasa la operación diaria que se da en la Facultad de Contaduría y Ciencias Administrativas.

Se realizó una investigación para examinar la situación actual de la Facultad de Contaduría y Ciencias Administrativas en cuanto a su equipo de cómputo existente. Uno de los puntos importantes que se trataron fue si se contaba con una cifra sobre el numero de incidentes que ocurren diariamente en dicha Facultad, y se obtuvo la siguiente grafica sobre los incidentes que ocurren diariamente, en promedio son 50 incidentes diarios, en diferentes tipos como software, hardware y periféricos.

Y se presentan en los siguientes porcentajes en la siguiente grafica:



Información obtenida por M.A. Rigoberto López Escalera encargado actualmente de departamento de cómputo de la Facultad de Contaduría y Ciencias Administrativas.

Formula:

$$\text{Improductividad} = \frac{\text{N. de computadoras}}{\text{N. de Incidentes}}$$

$$\text{Improductividad} = \frac{536}{50} = \mathbf{10.72\%}$$

La productividad implica eficacia y eficiencia en el desempeño individual y organizacional.

La formula nos arroja un 10.72% de improductividad diaria, en la Facultad de Contaduría Ciencias Administrativas, cifra que afecta de manera notable la operación que tiene dicha Facultad esto sin tomar en cuenta la acumulación de esta cifra por los incidentes que no son atendidos en su momento y que se acumulan a través del paso del tiempo, motivo por el cual es necesario administrar y controlar esta serie de situaciones, para que la operación no se vea afectada y cuenten tanto alumnos como docentes con el servicio informático disponible en todo momento.

Quizá sea un número que a simple vista no exprese mucho pero si tomamos en cuenta los recursos económicos, materiales y tiempo de espera, que se pierde con esta cifra no daremos cuenta que es urgente implementar una pronta solución a todo esto.

Una vez hecho todo el análisis anterior, se tienen los argumentos necesarios para solventar la presente tesis que propone la Creación de una Coordinación de Incidentes Informáticos, para que sea la responsable de corregir todos estos incidentes y ofrecer una pronta solución.

2. LA NECESIDAD DE CREAR UNA COORDINACION DE INCIDENTES INFORMATICOS.

Actualmente es importante llevar una administración exhaustiva en cada proceso que se realice en cualquier tipo de Institución o empresa, esto con la finalidad de optimizar y maximizar recursos materiales, humanos y económicos. Esta es una de las razones por la cual se propone la creación de la Coordinación de Incidentes Informáticos, y de esta manera administrar todo el recurso informático de la Facultad de Contaduría y Ciencias Administrativas.

Las necesidades de crear una Coordinación de Incidentes Informáticos son muchas y estas surgen a medida en que la demanda informática crece, esto aumenta al paso del tiempo ya que día con día es mas indispensable una computadora para hacer el trabajo diario más practico, rápido y seguro.

2.1 CUANTIFICACION DE LAS NECESIDADES DEL SERVICIO

Dentro de una empresa, el Centro de cómputo cumple diversas funciones que justifican los puestos de trabajo establecidos que existen en él, motivo por el cual es importante implementar una Coordinación de Incidentes Informáticos, para que cubra las siguientes necesidades.

- La Facultad requiere llevar un control sobre todos los incidentes informáticos.
- Es necesario que exista un registro sobre todas las anomalías que ocurren diariamente para en base a esto prever y evitar que continúen sucediendo.
- Es necesario poner fin al constante despilfarre informático que se da en la Facultad de Contaduría y Ciencias Administrativas.
- Al igual que todas las empresas e instituciones es necesario optimizar recursos en este caso recursos computacionales.
- Es importante que el usuario no pare sus actividades por incidentes que en ocasiones pueden ser solucionados en cuestión de algunos minutos.
- Es importante que el usuario cuente con un lugar donde se le brinde apoyo y asesoría técnica ya sea personal o vía telefónica dependiendo el caso.
- Es necesario aplicar esta nueva disciplina dentro de la Facultad de Contaduría y Ciencias Administrativas, por administración computacional dentro de la institución.
- Es necesario contar con personal especializado en lo que se refiere a la informática y dedicada únicamente a resolver incidentes informáticos.
- Es necesario eliminar incidentes conforme se vallan produciendo para no llegar a acumular una serie de fallas que juntas afecten a la institución de manera considerable.
- Es necesario optimizar recursos ya que ninguna empresa o institución esta en condiciones para despilfarrar recursos computacionales.
- Esta disciplina optimiza y maximiza recursos económicos, materiales y humanos.

2.2 CUANTIFICACION DE LAS VENTAJAS

Principales ventajas de la Coordinación de incidentes informáticos:

- El tiempo de interrupción del servicio informático se reduce, ya que existe ahora una administración de incidentes la cual ayuda a registrar y resolverlos.
- Es un nuevo procedimiento el cual tiene como objetivo reestablecer el servicio informático a la brevedad posible.
- El impacto de los incidentes indudablemente se reduce en un **50%** ya que ahora solo se concentran en un solo punto estratégico y se toman medidas correctivas en el momento que ocurre el incidente.
- Existe ahora una comunicación constante entre los usuarios y los técnicos.
- Se delegan responsabilidades.
- Existe ahora un control y registro, veraz y objetivo sobre lo que sucede con cada uno de los equipos de la Facultad de Contaduría y Ciencias Administrativas.
- Se analiza la información histórica y se toman decisiones preventivas.
- Se optimizan los recursos informáticos, obteniendo así la máxima utilidad de ellos.
- El capital humano da mejores resultados ya que ahora no existe un motivo informático, por el cual paren sus actividades por tiempo prolongado.
- Sin duda alguna administrar la función informática solo contraerá ventajas competitivas para la empresa o institución.
- Los directivos pueden contar con información veraz, oportuna en el momento que lo consideren ya que los procesos están controlados para que den los resultados esperados.

3. CREACION DE LA COORDINACION DE INCIDENTES INFORMATICOS

La creación de cualquier centro de cómputo no es tarea fácil ni sencilla, se deben de tomar ciertas pautas al momento de hacer la elección, ya que las necesidades de cada centro de cómputo son distintas ya sea en cuanto a software, hardware, personal, mobiliario, etc.

La creación de la Coordinación de Incidentes Informáticos, no será la excepción sus funciones serán muy especificas y diferentes a las de cualquier otro centro de computo ya existente, razón por la cual se debe hacer primero un análisis sobre la operación que se realizara en la Coordinación de Incidentes Informáticos, y en base a esto se tomarán las decisiones sobre el tipo de hardware, software, mobiliario y personal.

Todo estudio determina una configuración mínima la computadora y los aditamentos o dispositivos electrónicos anexos como unidades externas, impresoras, tarjetas y modems para comunicaciones, elementos para backups, etc. De acuerdo con las necesidades del usuario, así como una evaluación del costo aproximado de la inversión.

3.1 ANALISIS SOBRE LAS NECESIDADES DE HARDWARE Y SOTFWARE DE LA CII

La Coordinación de Incidentes Informáticos, es un centro de cómputo cuya tarea va ser registrar, controlar y resolver todas las anomalías que se presenten en la Facultad de Contaduría Ciencias Administrativas.

Para comenzar el análisis cabe mencionar que no estamos hablando de centro de cómputo grande, en realidad para la función que va realizar no es necesario consolidarlo de esa forma, esta crecerá conforme lo demanden las necesidades la Facultad de Contaduría Ciencias Administrativas.

La Coordinación de Incidentes Informáticos, estará conformada por cinco computadoras las cuales solventaran las necesidades del lugar, una red entre ellas, el software que permita realizar diferentes tipos de tareas necesarias dentro del mismo y el personal suficiente para operar.

La selección del hardware y software requerido para nuestro proyecto, debe ir de acuerdo a un plan estratégico y sustentado por un estudio elaborado previamente, en el cual se enfatizan las características y volumen de información que ameritan sistematización y diferencian los tipos de equipos que se adjudican a las diversas áreas usuarias.

Para realizar cualquier adquisición de software o hardware, se deberán considerar los siguientes puntos:

- Solicitud de propuesta. Todo sistema se origina en base a una solicitud que hace el usuario al centro de cómputo, intentando satisfacer una necesidad especifica.

  Los parámetros sobre los cuales debe medirse dicha solicitud son los objetivos y las políticas, los cuales debe fijar el usuario, aunque puede ser que el departamento de análisis le brinde ayuda en su clarificación. Ambos parámetros deben quedar establecidos por escrito.
- Evaluación de propuesta. Previamente debe llevarse a cabo una investigación con el propósito de establecer con seguridad el tipo de software y hardware requerido para su implementación, posteriormente se integra toda la información obtenida de dicha investigación y así poder establecer la operatividad de los sistemas a adquirirse.
- Financiamiento. Las fuentes de financiamiento pueden ser principalmente instituciones bancarias a través de créditos. Para el caso de centros de cómputo destinados a la educación pública no existen fuentes de financiamiento, a menos que la institución educativa cuente con un área destinada a la producción de software para empresas privadas, entonces la misma empresa puede ser el origen del financiamiento.
- Negociación de Contrato. La negociación de contrato debe incluir todos los aspectos de operación del software y del hardware a implementarse. Aspectos tales como: Actualizaciones, innovaciones, capacitación, asesoría técnica, etc.

  Permisos y Licencias.

  El uso de software no autorizado o adquirido ilegalmente, se considera como pirata y una violación a los derechos de autor.

3.2 ADOPCION DEL NUEVO HARDWARE

El hardware dentro de la empresa o institución es un activo muy valioso e importante, razón por la cual se debe de tener un especial cuidado en el momento de adquirirlo, se deben tomar en cuenta las necesidades del lugar donde este vaya a funcionar, y en base a esto hacer una buena elección de hardware.

La Coordinación de Incidentes Informáticos de la Facultad de Contaduría Ciencias Administrativas, es un centro de cómputo el cual estará conformado de la siguiente manera.

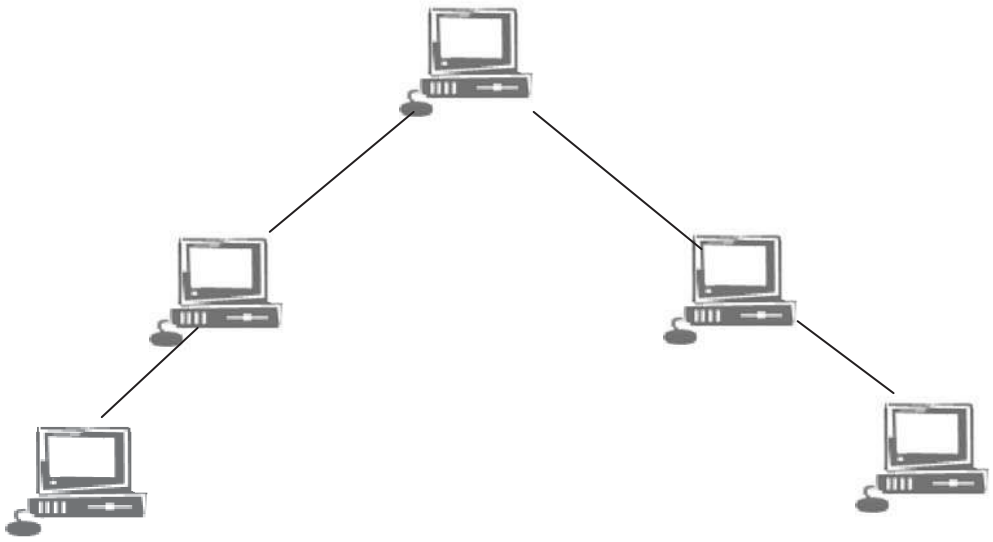
Cinco computadoras con las siguientes características:
Monitor LCD 15”
Memoria Ram 512mb
Disco duro 120Gb
Procesador Intel Pentium 4 3.6ghz
Mouse óptico
Teclado 105 teclas
Combo Dvd 16x
Un interruptor No break (baterías ó pilas)
Impresora
Regulador

ESTRUCTURA DE LA COORDINACION DE INCIDENTES INFORMATICOS

Topología árbol:

En esta topología que es una generalización del tipo bus, el árbol tiene su primer nodo en la raíz y se expande hacia fuera utilizando ramas, en donde se conectan las demás terminales.

Esta topología permite que la red se expanda y al mismo tiempo asegura que nada más existe una ruta de datos entre dos terminales cualesquiera.



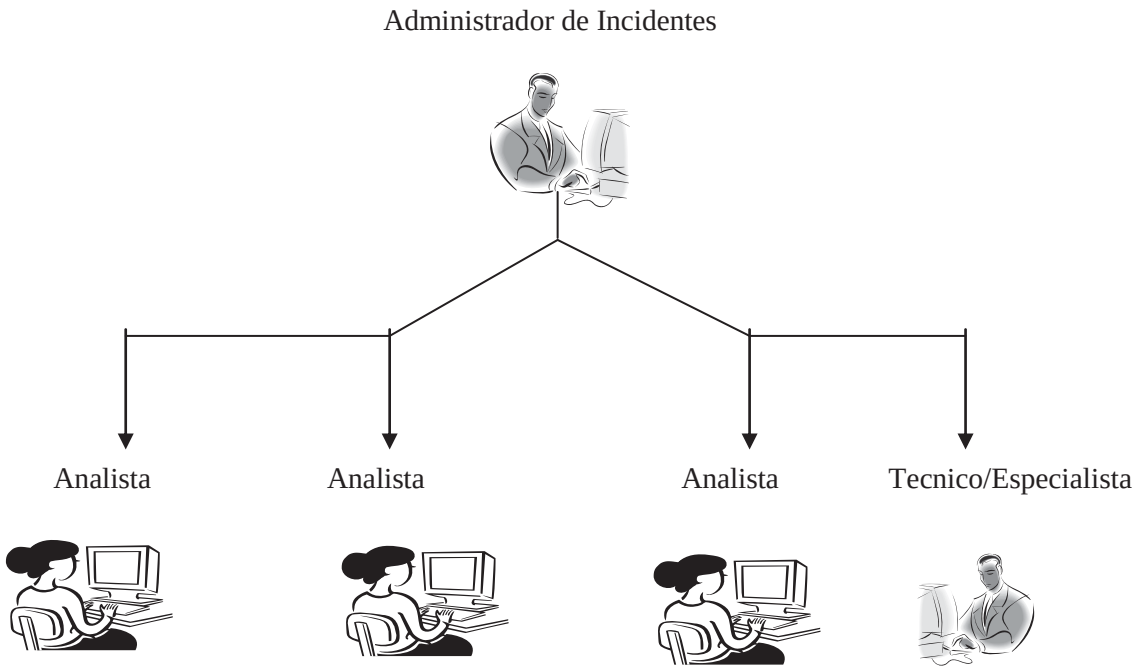
Como se pude apreciar la Coordinación de Incidentes Informáticos, es un Centro de Cómputo pequeño, lo que refleja como con poca inversión y una buena administración se puede optimizar recurso económico como computacional, que es lo que pretende el presente proyecto.

La distribución de cada una de estas será de la siguiente manera:

1 equipo de cómputo, para el administrador de incidentes informáticos (Servidor)

3 equipo de cómputo, para los analistas

1 equipo de cómputo, para las necesidades extras del técnico



3.3 ADOPCION DEL NUEVO SOFTWARE

Software: Conjunto de programas o listas de instrucciones codificadas los cuales le permiten a la computadora realizar una o varias funciones.

El software dentro de cualquier institución o empresa, es la herramienta que nos permite realizar diferentes tipos de tareas, existe software general y software especifico, al momento de adquirir cualquiera de los dos tipos de software, se debe analizar las necesidades de la empresa y tener especial cuidado en ciertos criterios, como los siguientes:

- Reconocido prestigio mundial y nacional.
- Soporte técnico en instalación.
- Ayuda en problemas.
- Personal especializado.
- Tiempo de atención.
- Comunicación rápida.
- Servicios de capacitación: cursos, material, expositor, costos.
- Cartera de clientes de software iguales al adquirido.
- Documentación: Facilidad de uso.

Una vez visto esto se debe hacer la lista de requerimientos según el lugar para el que se va a adquirir el software existen ciertos paquetes básicos como son:

- Office 2007
- Adobe reader
- Nero Express 2007
- Traductor
- Antivirus

En nuestro caso será necesario adquirir un software específico, con la finalidad de manejar la información de acuerdo a las necesidades de, **la Coordinación de Incidentes Informáticos**.

Al momento de hablar de un software específico estamos hablando de una herramienta que estará diseñada a la medida de las necesidades del lugar, en nuestro caso de la Coordinación de Incidentes Informáticos.

Este tipo de software en la actualidad son sistemas muy ligeros que ayudan a realizar el trabajo de una manera fácil, práctica y que de igual forma puede manejar nuestra información de forma segura y confiable.

Este tipo de software lo diseñaremos mas adelante de acuerdo a la manera en que trabajaremos la información, únicamente requeriremos de un software específico y de software general, los ya mencionados anteriormente.

3.4 ANÁLISIS Y DISEÑO DE UN SISTEMA DE OPERACIÓN.

En el tema 3.3 se describió sobre los tipos de software específicos y generales que ocupa cualquier empresa o institución para facilitar las diferentes tareas que deben de realizar cotidianamente, para cumplir con los objetivos de cada área o departamento, en este tema hablaremos sobre el análisis y diseño de un software especifico.

Un software específico sabemos que es aquel que esta diseñado de acuerdo a las necesidades y características de determinado lugar y este funciona para automatizar la información y poder disponer de ella de manera oportuna y concreta en todo momento. Este tipo de software se crea y diseña, realizando un análisis muy exhaustivo sobre la información que requiere recopilar el usuario, para posteriormente utilizarla a favor lo objetivos del área o departamento.

La Coordinación de Incidentes Informáticos, requiere de un sistema de operación que este diseñado de acuerdo a las necesidades del servicio que prestará, como es la captura de Incidentes Informáticos, para esto es necesario realizar un análisis sobre las necesidades y características que debe tener el sistema que utilizara dicho departamento, para automatizar la información y poder concentrarla de manera concreta y correcta, con esto poder disponer de la información de los incidentes que se registren en forma ordenada, veraz y oportuna en todo momento.

Para solicitar el sistema de operación, únicamente se realizara el análisis y diseño de este, la programación y la implementación lo realizara el personal encargado de desarrollo de software de la Universidad Michoacana de San Nicolás de Hidalgo, ubicados en el edificio N de la ciudad universitaria, el sistema de operación será para gestionar lo que es la recepción, transición y solución de Incidentes Informáticos.

Análisis sobre el sistema de operación

El sistema debe cubrir las siguientes características:

Recepción del incidente

Número de incidente: Referente a la secuencia y conteo de los incidentes que se registren, este número de incidente se le debe otorgar al usuario como referencia y seguimiento de su llamada y reporte del incidente informático.

Número de empleado o matricula: El usuario debe identificarse con su número de empleado o matricula, para poder disponer de la ayuda de la Coordinación de Incidentes Informáticos, solo usuarios activos están autorizados para el uso de laboratorios de la Facultad.

Nombre completo del usuario: Es importante obtenerlo, para saber a quien dirigirnos en un momento determinado.

Área afectada: En este campo determina el analista receptor del incidente, el área que ha sido afectada puede ser software, hardware, redes, impresoras, Internet, etc.

Nivel de asignación: Una vez que el analista registra el incidente lo ubica en un nivel de atención, si en su momento el analista lo soluciono, entonces en este campo deberá seleccionar análisis de no ser así pasara a ser atendido por los siguientes niveles como especialistas o jefes de departamento.

Nombre de la persona responsable del incidente: En este campo se destinará a la persona responsable de la resolución del incidente en determinada escala que fuese.

Descripción del incidente: En este campo se anotará la descripción sobre el incidente informático que el usuario reporta.

Acciones realizadas: Una vez que se atendió en alguna de los tres niveles, la persona a la que se le asigno el incidente deberá anotar una breve reseña sobre las acciones que realizo para la resolución del incidente.

Estado actual del incidente: En este campo se deberá señalar el estado actual del incidente Informático, podrá estar en tres diferentes tipos de estados como;
Abierto: El analista en el momento que abre un incidente deberá seleccionar esta opción.
Transición: Una vez que la persona a la que fue asignado determinado incidente toma el reporte deber cambiar la opción de abierto a transición esto denotara que el incidente esta siendo atendido.
Solución: Una vez que la persona a quien fue asignado determinado incidente, lo haya resuelto entonces deberá cambiar la opción en el reporte de transición a solución y con esto el reporte se tomara como atendido y cerrado.

Tiempo de atención: Siempre que un usuario se comunique a la Coordinación de Incidentes Informáticos, en el momento en que se abre el incidente comenzara un reloj que tomara el tiempo de atención, esté únicamente se tomara como referencia para efectos de calidad en el servicio.

Hora y fecha de registro: Datos muy importantes para cualquier tipo de captura, este dato nos servirá desde luego para tomar referencias en determinado momento que lo requiera cada situación.

Buscar en la base del conocimiento: Este campo es muy importante y de mucha ayuda para la Coordinación de Incidentes Informáticos, ya que todas las personas que solucionen algún incidente, deberán ingresar a la base de datos del conocimiento y realizar un registro sobre los pasos a seguir para solucionar cierto incidente, esto ayudará a que con el paso del tiempo los analistas logren solucionar vía telefónica los incidentes que sean teóricos y de esta manera dar una atención rápida y efectiva a los usuarios de la Facultad de Contaduría Ciencias Administrativas.

Guardar: Este icono se utilizara para guardar el incidente una vez que haya sido completamente llenado

Cancelar: Este icono se utilizara una vez que se halla guardado el incidente y el usuario vuelva a llamar para solicitar su cancelación.

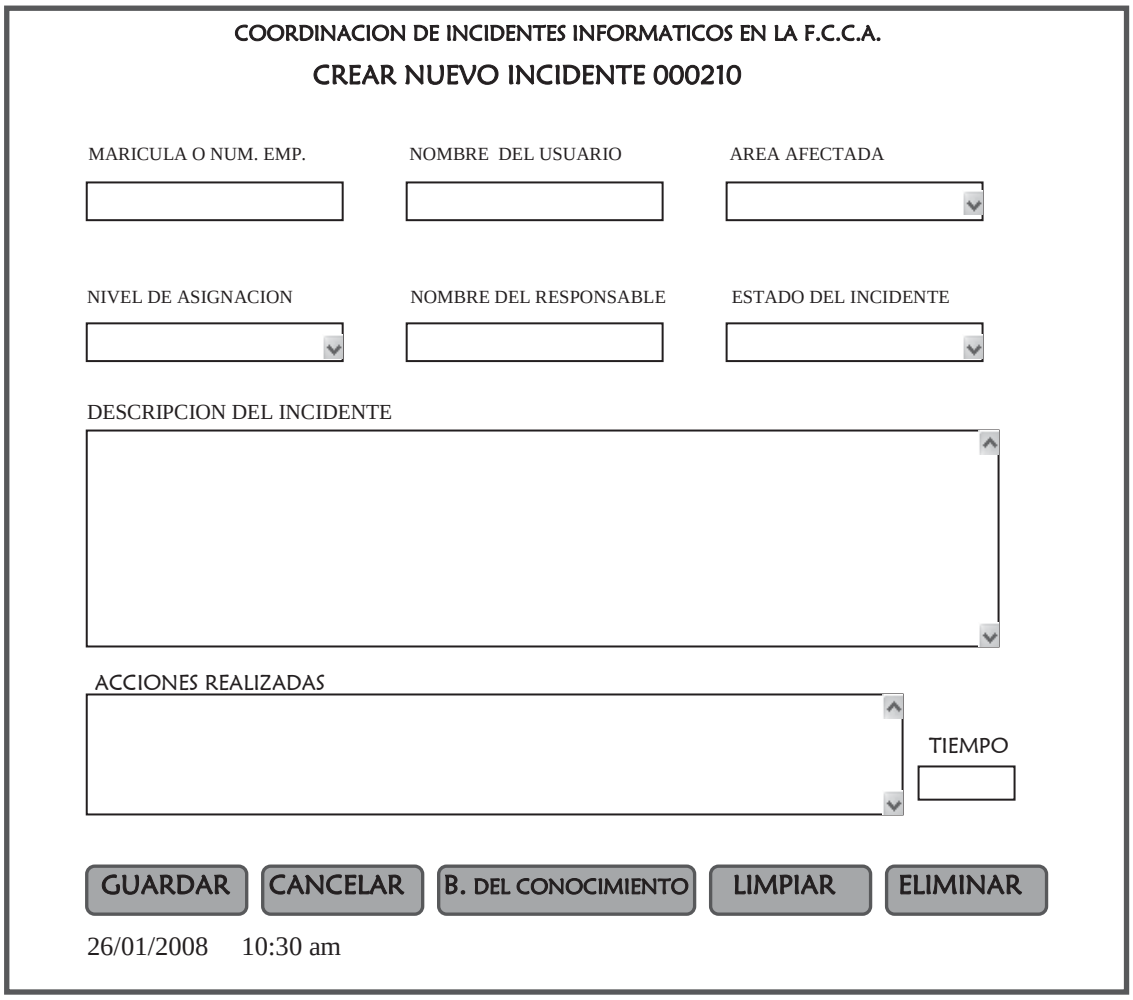
Limpiar: Este icono ayuda a analista una vez que lleno todo los requisitos para la apertura de un incidente y el usuario decide no aperturarlo, únicamente con presionar este icono la información registrada se borrara y el incidente abierto se podrá usar para otro que se quiera registrar.

Eliminar: Una vez que el incidente ya fue atendido y resuelto únicamente el analista y el administrador de Incidentes, tendrán privilegios para eliminarlos de la base de datos de Incidentes Informáticos.

Todos los puntos anteriores es información muy importante para la Coordinación de Incidentes Informáticos, ya que cada uno de esos datos nos ayudara a tener un registro y control absoluto sobre los incidentes informáticos que registraran.

Diseño sobre el sistema de operación

El diseño del esquema o bien la tabla de captura para el registro de Incidentes Informáticos sería de la siguiente manera:



EJEMPLO DE UN REPORTE SOBRE UN INCIDENTE INFORMATICO

COORDINACION DE INCIDENTES INFORMATICOS EN LA F.C.C.A.

CREAR NUEVO INCIDENTE 000210

MARICULA O NUM. EMP.	NOMBRE DEL USUARIO	AREA AFECTADA
9903511K	KARINA ISABEL TORRES PONCE	SOFTWARE

NIVEL DE ASIGNACION	NOMBRE DEL RESPONSABLE	ESTADO DEL INCIDENTE
ESPECIALISTAS	PABLO GONZALEZ CHAVEZ	ABIERTO

DESCRIPCION DEL INCIDENTE

El día de hoy, por la mañana la maquina numero 12 de laboratorio 4 del Edificio Y, se encontraba sin algunos programas entre ellos:
Office, photoshop y corel
Programas que requiere forzosamente el usuario para diferentes materias que cursa actualmente.

ACCIONES REALIZADAS

TIEMPO 02:30

GUARDAR | CANCELAR | B. DEL CONOCIMIENTO | LIMPIAR | ELIMINAR

26/01/2008 10:30 am

EJEMPLO DE UN REPORTE SOBRE UN INCIDENTE INFORMATICO

COORDINACION DE INCIDENTES INFORMATICOS EN LA F.C.C.A.

CREAR NUEVO INCIDENTE 000210

MARICULA O NUM. EMP.	NOMBRE DEL USUARIO	AREA AFECTADA
9903511K	KARINA ISABEL TORRES PONCE	SOFTWARE

NIVEL DE ASIGNACION	NOMBRE DEL RESPONSABLE	ESTADO DEL INCIDENTE
ESPECIALISTAS	PABLO GONZALEZ CHAVEZ	ABIERTO

DESCRIPCION DEL INCIDENTE

El día de hoy, por la mañana la maquina numero 12 de laboratorio 4 del Edificio Y, se encontraba sin algunos programas entre ellos:
Office, photoshop y corel
Programas que requiere forzosamente el usuario para diferentes materias que cursa actualmente.

ACCIONES REALIZADAS

Se instalaron los programas requeridos y el usuario retomo actividades.

TIEMPO 04:00

GUARDAR | CANCELAR | B. DEL CONOCIMIENTO | LIMPIAR | ELIMINAR

26/01/2008 10:30 am

3.5 UBICACIÓN FISICA Y MOBILIARIO

La ubicación física e instalación de un Centro de Cómputo en una empresa depende de muchos factores, entre los que podemos citar: el tamaño de la empresa, el servicio que se pretende obtener, las disponibilidades de espacio físico existente o proyectado, etc. Generalmente, la instalación física de un Centro de Cómputo exige tener en cuenta por lo menos los siguientes puntos:

- Local físico. Donde se analizará el espacio disponible, el acceso de equipos y personal, instalaciones de suministro eléctrico, acondicionamiento térmico y elementos de seguridad disponibles.
- Espacio y movilidad. Características de las salas, altura, anchura, posición de las columnas, posibilidades de movilidad de los equipos, suelo móvil o falso suelo, etc.
- Iluminación. El sistema de iluminación debe ser apropiado para evitar reflejos en las pantallas, falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos.
- Tratamiento acústico. Los equipos ruidosos como las impresoras con impacto, equipos de aire acondicionado o equipos sujetos a una gran vibración, deben estar en zonas donde tanto el ruido como la vibración se encuentren amortiguados.
- Seguridad física del local. Se estudiará el sistema contra incendios, teniendo en cuenta que los materiales sean incombustibles (pintura de las paredes, suelo, techo, mesas, estanterías, etc.). También se estudiará la protección contra inundaciones y otros peligros físicos que puedan afectar a la instalación.
- Suministro eléctrico. El suministro eléctrico a un Centro de Cómputo, y en particular la alimentación de los equipos, debe hacerse con unas condiciones especiales, como la utilización de una línea independiente del resto de la instalación para evitar interferencias, con elementos de protección y seguridad específicos y en muchos casos con sistemas de alimentación ininterrumpida instalación de baterías.

LOCALIZACIÓN DEL LUGAR PARA LA COORDINACIÓN DE INCIDENTES INFORMÁTICOS

Se ha pensado en un posible lugar a tomar en cuenta para la instalación de la Coordinación de Incidentes Informáticos, esté es dentro del edificio A-2, en la planta baja, a un costado del laboratorio 3, de la Facultad de Contaduría y Ciencias Administrativas, el mobiliario como el hardware que se implementara, ocupara poco espacio, sin embargo se deberán tomar algunos criterios importantes sobre la seguridad en el espacio físico para la instalación de dicho Departamento.

Las características son las siguientes:

- ✓ El área deberá medir por lo menos 4*4 m^2
- ✓ No deberá haber muchas ventanas.
- ✓ El área no deberá contar con lámparas u objetos colgantes que puedan dañar el hardware en caso de siniestros.
- ✓ El lugar deberá estar no más de 35 ºC o menos de 10ºC.
- ✓ Deberá ser fresco y donde pueda circular bien el aire.
- ✓ Deberá existir un área despejada que permita el fácil acceso y la rápida evacuación en caso de siniestros.
- ✓ Deberá tener cercanía a usuarios potenciales.
- ✓ Será necesario contar con buenos servicios de comunicación.
- ✓ De ser requerido se instalará un detector de humo el cual nos indicara en caso de haber un corto circuito u otro que se le parezca.
- ✓ Deberá contar con conexión a tierra física.

Todo esto será con la finalidad de que el área sea lo mas segura posible, para evitar daños al hardware, software y mobiliario, y que este pueda proporcionar un servicio eficiente y de calidad en todo momento.

REQUERIMIENTOS DE MOBILIARIO

El mobiliario así como la papelería de oficina es un activo muy importante, para poder operar en cualquier departamento, los requerimientos de estos tienen que tener una razón ser, y es importante analizar que realmente es necesario para el departamento, ya que solo de esta manera no se harán gastos insuficientes en cosas que probablemente no son necesarias.

El mobiliario necesario para poder operar como Coordinación de Incidentes Informáticos será el siguiente:

REQUERIMIENTO DE MOBILIARIO	JUSTIFICASION	PRECIO UNI.	TOTAL
4 Computadoras	Para operar los analistas y técnicos.	6,999.00	27,996.00
1 servidor	Para operar el administrador de incidentes informáticos.	13,899.00	13,899.00
Costo total de Software (office, nero, antivirus, traductor, adobe reader)	Para desarrollar diferentes tipos de tareas en la Pc.	7,400.00	7,400.00
1 Impresora	Para la impresión de formatos o reportes que requiera la C.I.I.	4,499.00	4,499.00
7 Reguladores	Para regular las descargas de energía eléctrica.	89.00	623.00
6 Mesas	Sobre cada mesa se colocaran 1 computadora.	399.00	2,394.00
6 Sillas	Uso exclusivo del personal de la Coordinación.	375.00	2,250.00
6 Teléfonos	Para recibir llamadas respecto a incidentes informáticos.	229.00	1,374.00
5 Diademas telefónicas	Esto para que los operadores tengan las manos libres y puedan levantar el reporte en la Pc.	89.00	445.00
1 Extinguidor	Esto por cualquier siniestro que pudiera llegar a ocurrir.	499.00	499.00
2 Botes de basura	Para la basura que sale por la operación cotidiana.	79..00	158.00
1 Ventilador	En caso de que se caliente el lugar por el numero de Pc´s.	719.00	719.00
Total			$62,256.00

La papelería que se requiere para la operación diaria de la Coordinación de Incidentes Informáticos es la siguiente:

REQUERIMIENTO DE PAPELERIA	RAZON	COSTO UNI	TOTAL
10 Paquete Hojas	Para uso exclusivo de la Coordinación, impresiones , escritos, etc.	50.00	500.00
1 Pintarrón	Para notas importantes de la Coordinación.	299.00	299.00
2 Paquete Plumones para pintarrón	Para anotar en el pintarrón datos relevantes.	49.00	98.00
160 Carpetas	Para documentos que se requieran archivar.	31.00	124.00
8 Carpetas blancas	Para archivar y ordenar documentación histórica.	49.00	392.00
4 Paquete Lapiceros y lápices	Para trabajar durante el día.	18.00	72.00
1 Archivero	Para guardar documentos importantes	2,762.00	2,762.00
total			$4,247.00

SE ESTIMA UN MONTO APROXIMADO EN EQUIPO DE COMPUTO, PAPELERIA Y MOBILIARIO DE **$ 66,503.00** *

Estos son requerimientos y costos que implican la adquisición de los recursos de mobiliario y papelería necesarios, para operar la Coordinación de Incidentes Informáticos.

*(cotización realizada en noviembre 2007)

4. FUNCIONALIDAD DE LA COORDINACION DE INCIDENTES INFORMATICOS

La funcionalidad de la Coordinación de Incidentes Informáticos (en adelante C.I.I.) será dar apoyo a todos los usuarios que soliciten su ayuda, esta Coordinación esta consolidada como un centro de primer impacto a donde todos los usuarios tendrán que recurrir en el momento que sufran algún tipo de interrupción del servicio informático.

La funcionalidad esta diseñada de la siguiente manera:

INTERRUPCION INFORMATICA

- El usuario se comunica vía telefónica a C.I.I
- El usuario acude personalmente a C.I.I.
- El usuario envía un correo electrónico C.I.I.

Posteriormente se llevara a cabo el procedimiento ya establecido en la Coordinación de Incidentes Informáticos.

4.1 DESCRIPCION DE ACTIVIDADES

Las actividades a desarrollar dentro de la Coordinación de Incidentes Informáticos, serán los siguientes:

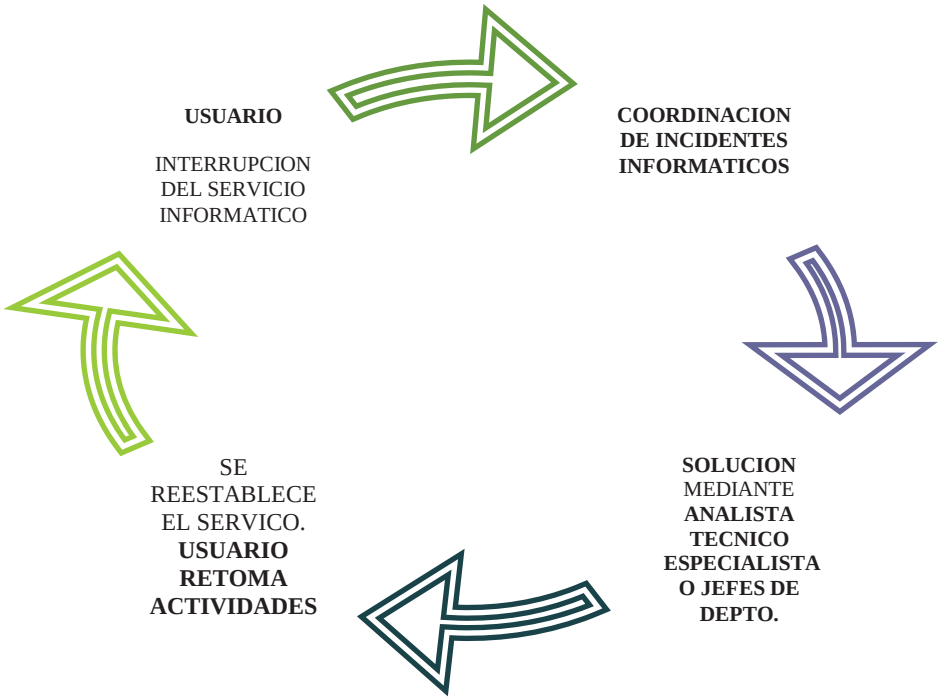
- ✓ Atención telefónica y registro de incidentes en la base de datos.
- ✓ Tipificación de incidentes
- ✓ Monitoreo constante al sistema de la C.I.I. donde se ingresan todos los incidentes con el fin de dar seguimiento puntual a cada incidente.
- ✓ Generación de estadística diaria de incidentes.
- ✓ Mantener informado al Administrador de Incidentes Informáticos cuando existan dos o más reportes sobre un mismo incidente.
- ✓ Mantenimiento preventivo y correctivo por parte de los técnicos a todo el equipo de cómputo de la Facultad de Contaduría Ciencias Administrativas.
- ✓ Dar solución a la brevedad posible sobre los incidentes de primer nivel
- ✓ Dar solución por medio de los especialista a los incidentes de segundo nivel
- ✓ Dar solución a los incidentes de tercer nivel, tomando una decisión con los directivos.
- ✓ Resolver todos los incidentes que tengan relación con hardware, software, redes, Internet, impresoras, copiadoras, fax.
- ✓ Realizar auditorias de software y hardware en los diferentes laboratorios y lugares donde exista equipo de cómputo de la facultad.
- ✓ Administrar todo el recurso informático correctamente.

Las actividades anteriores las desarrollarán personal capacitado y preparado para poder dar un servicio de calidad y que finalmente nos arroje el resultado que estamos buscando, que es el de administrar correctamente la operación Informática de la Facultad de Contaduría Ciencias Administrativas.

La operación se puede apreciar de la siguiente manera:

INTERRUPCION INFORMATICA

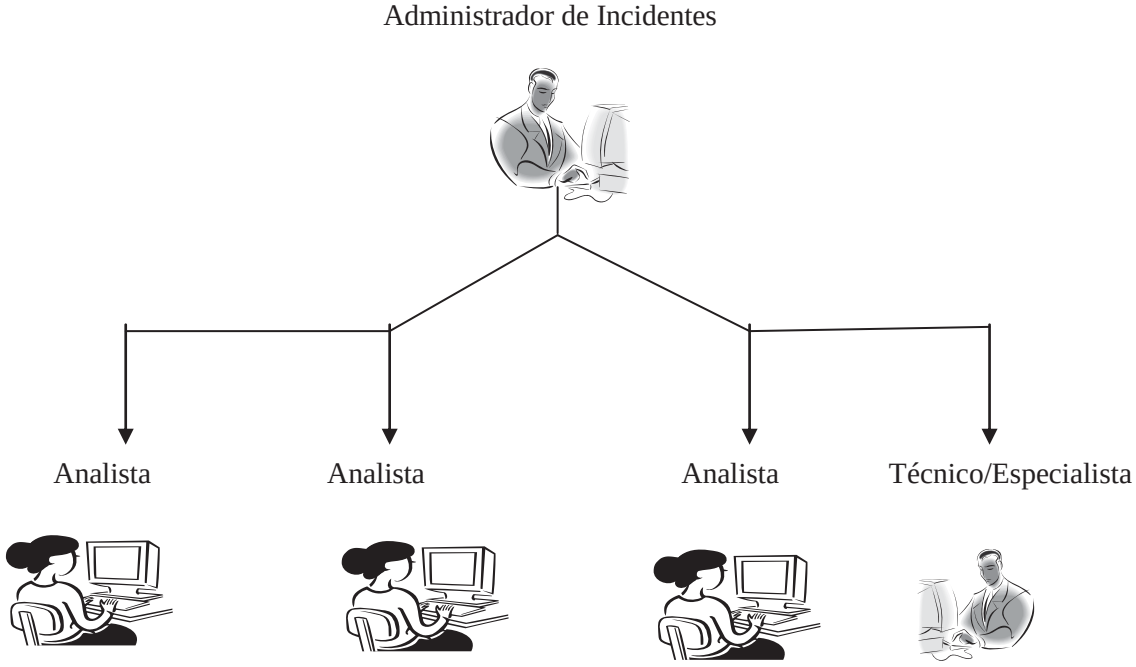
- El usuario se comunica vía telefónica a C.I.I.
- El usuario envía un electrónico C.I.I.
- El usuario levanta el reporte personalmente en C.I.I.



4.2 ESTRUCTURA DE LA COORDINACION DE INCIDENTES INFORMATICOS

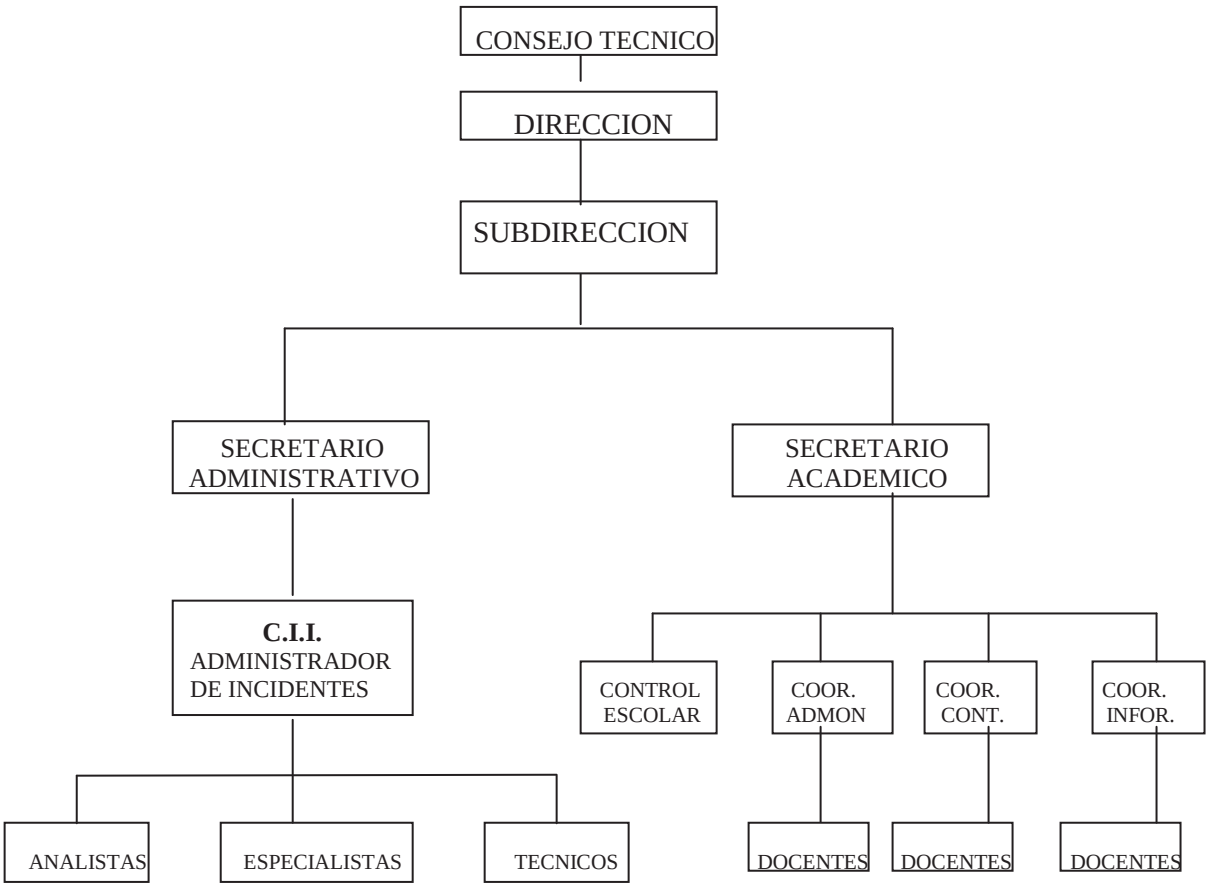
La Coordinación de Incidentes Informáticos, cuenta con un administrador de incidentes, persona responsable de todo el departamento, tres analistas personas que se encargaran de atender todas las llamadas solucionar incidentes vía telefónica o bien canalizarlos con el técnico o especialista, dos técnicos responsables de atender todos los incidentes que les sean asignados, respecto a los especialistas únicamente se trabajara con ellos en coordinación cuando algún sistema sufra alguna falla ya que ellos se encuentran ubicados en el edificio N y son los responsables de los sistemas con los que trabaja la Universidad Michoacana de San Nicolás de Hidalgo.

La estructura de la Coordinación de Incidentes Informáticos se conforma de la siguiente manera:



4.3 ESTRUCTURA ORGANIZACIONAL EN LA FACULTAD DE CONTADURIA Y CS ADMINISTRATIVAS

La Facultad de Contaduría y Ciencias Administrativas, cuenta con un organigrama vertical encabezado por el Consejo Técnico de dicha Facultad seguido de el siguen el director, en lo sucesivo se va desplegando una serie de departamentos necesarios para el buen funcionamiento de esta Institución, el organigrama lo podemos apreciar a continuación.



4.4 ACTIVIDADES Y RESPONSABILIDADES

Las actividades y responsabilidades que deberán desempeñar cada uno de los integrantes de la Coordinación de Incidentes Informáticos, son muy importantes y delimitantes al mismo tiempo, enseguida describiremos cada una de las actividades que realizaran cada uno de los puestos que integran la Coordinación de Incidentes Informáticos.

Administrador de incidentes: Se refiere a la persona responsable de administrar todos los Incidentes que se registran en la Coordinación de Incidentes Informáticos, de la Facultad de Contaduría y Ciencias Administrativas. Así como organizar al personal y delegar actividades a desarrollar dentro de la Coordinación de Incidentes Informáticos, verificar que estos cumplan con las responsabilidades, normas y políticas correspondientes.
Elaboración de informes sobre:

- Incidentes más frecuentes.
- El desempeño de la Coordinación de Incidentes Informáticos.
- Incidentes no resueltos.
- Nuevas soluciones identificadas.
- Analizar los incidentes correspondientes a los servicios informáticos a su cargo, documentarlos y registrarlos de manera clara y precisa, para que en lo sucesivo la información pueda ayudar a describir, diagnosticar y encontrar una solución en primer nivel a cada incidente.
- Tomar acciones necesarias para que el personal a su cargo cumpla con el procedimiento establecido y resuelvan los incidentes en los tiempos de atención establecidos.
- El administrador de incidentes informáticos entra en procedimiento en el tercer nivel cuando una vez escalado los niveles anteriores no obtuvo el incidente una respuesta satisfactoria, entonces el administrador de incidentes en colaboración con los jefes de departamento toman una solución temporal o definitiva.

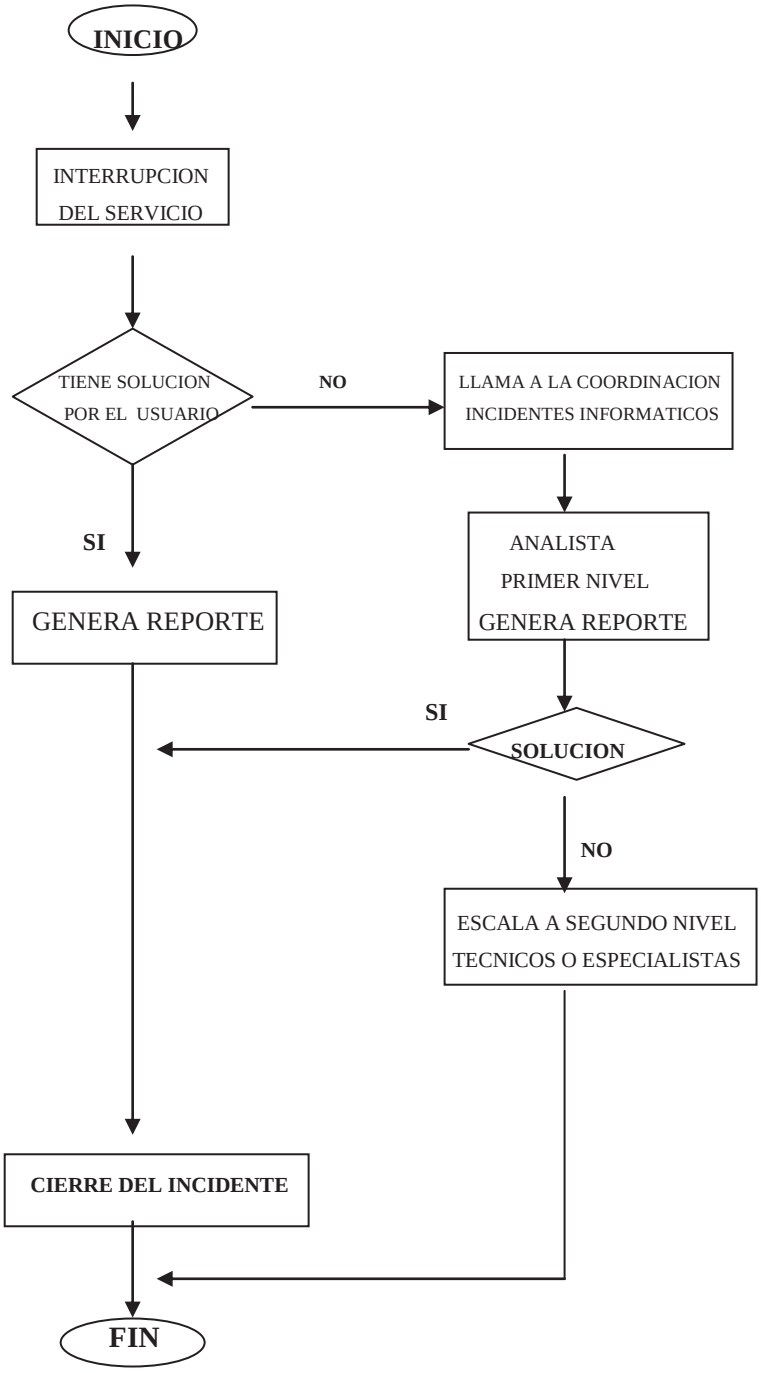
Analistas: Son las personas encargadas de contestar todas las llamadas, revisar el correo electrónico de la Coordinación Incidentes Informáticos, y atender a los usuarios que soliciten el servicio de atención de la C.I.I., por algún incidente que se les presento, el analista tiene la responsabilidad de recibir la llamada, levantar el reporte, y si en la base de datos sobre incidentes resueltos, esta ya documentada la solución de incidente que le esta presentando el usuario, entonces, el analista orienta al usuario buscando una pronta solución, si esta no es satisfactoria el analista entonces lo escala a segundo nivel con un técnico o especialista según sea el caso, para que estos le den seguimiento al incidente hasta resolverlo.

La función y procedimiento del analista es el siguiente:
Analista recibe la llamada del usuario que solicita el servicio de apoyo para resolver un incidente que se le suscito, el analista apoyándose del software servicio de incidentes, comienza a levantar el reporte, identifica al usuario ingresando su matricula o numero de empleado para buscarlo en la base de datos, una vez que es identificado, pregunta en que le puede ayudar, posteriormente levanta el reporte y lo resuelve si esta la solución a su alcance, ó en su defecto lo escala a segundo nivel, le otorga al usuario un numero de reporte para dar seguimiento a este, el usuario una vez que el incidente sea resuelto deberá comunicarse a la Coordinación de Incidentes Informáticos dar el numero de reporte y autorizar el cierre del mismo satisfactoriamente.
En caso de que el incidente sea resuelto en primer nivel, el analista deberá completar la información necesaria para documentar la solución del incidente y cerrar el incidente.

Mantener comunicados a los usuarios y a sus colaboradores de los avances, atrasos y problemas que se presentan rutinariamente y cuando sea necesario a través de medios establecidos formalmente, como el uso de correo electrónico.

Los analistas tienen la función de establecer un flujo de información eficiente a través de toda la facultad.

El procedimiento se puede apreciar de la siguiente manera en el diagrama de flujo:



Técnicos: Son las personas responsables de la gestión del hardware y del software dentro de las instalaciones de la Facultad de Contaduría Ciencias Administrativas, entendiendo por gestión: estrategia, planificación, instalación y mantenimiento.

La Coordinación de Incidentes Informáticos, cuenta con técnicos, personal capacitado para atender todos los incidentes que le sean asignados por la C.I.I. la función de los técnicos será pasar personalmente a lugar del incidente informático para resolverlo, trátese de hardware, software, redes, etc. este personal esta enfocado a atender todos los incidentes que requieren atención personalizada.

Algunas funciones principales generales que realizan los técnicos son:

- Atender todos los incidentes que le sean asignados única y exclusivamente por C.I.I.
- Planificar la modificación e instalación de nuevo software y hardware.
- Evaluar los nuevos paquetes de software y nuevos productos de hardware.
- Dar el soporte técnico necesario para el desarrollo de nuevos proyectos, evaluando el impacto de los nuevos proyectos en el sistema instalado.
- Asegurar la disponibilidad del sistema, y la coordinación necesaria para la resolución de los problemas técnicos en su área.
- Realizar la coordinación con los técnicos del proveedor con el fin de resolver los problemas técnicos y garantizar la instalación de los productos.
- Proponer las notas técnicas y recomendaciones para el uso óptimo de los sistemas instalados.
- Documentar el reporte de incidente, notificando las acciones que hallan realizado para resolverlo.

Especialistas: Son considerados en este caso como, las personas encargadas de la programación de sistemas, se encargan de elaborar los programas o bien el software especifico que requiere la Facultad de Contaduría Ciencias Administrativas, modifican los existentes y vigilan que todos los procesos se ejecuten correctamente.

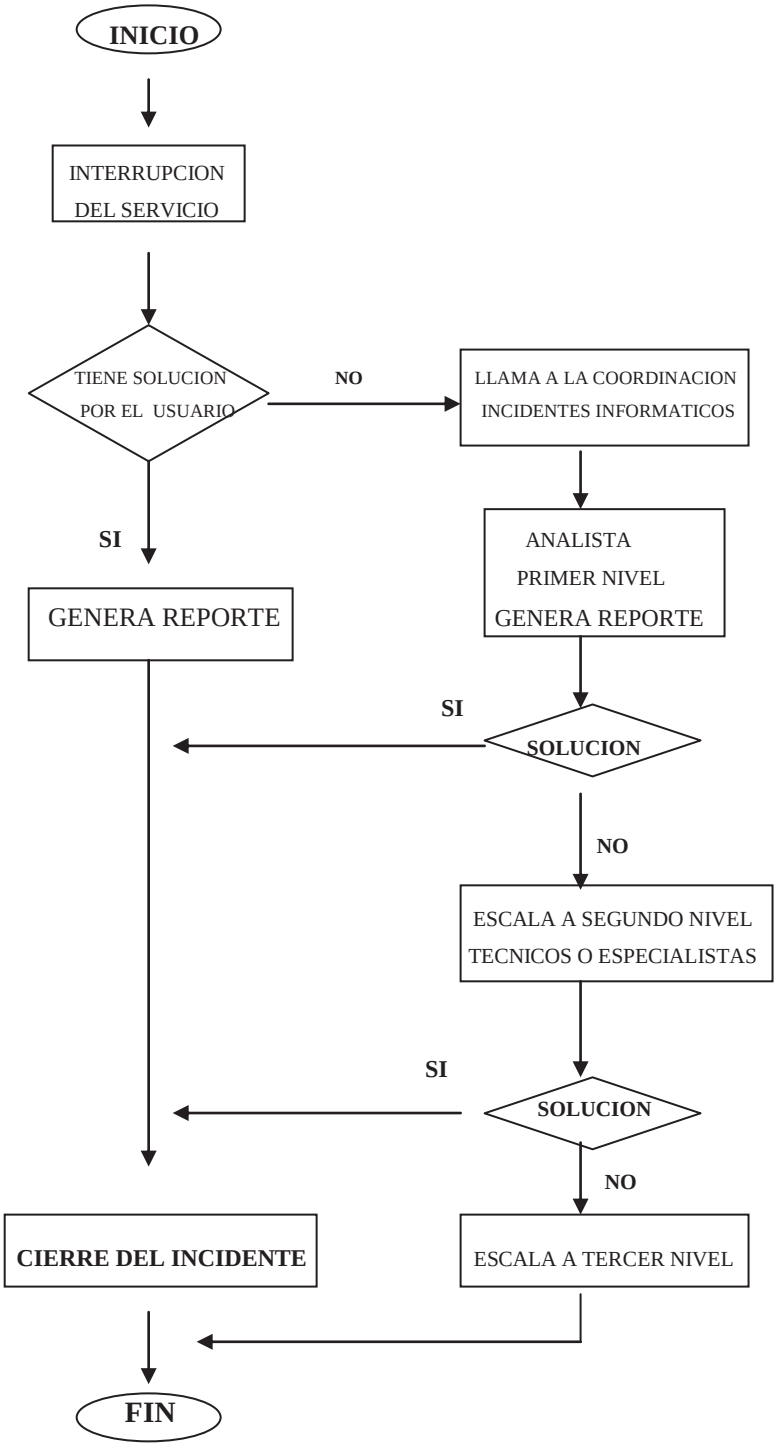
Los programadores de sistemas deben tener los conocimientos suficientes del hardware para poder optimizar la utilización del equipo. Su función es extremadamente técnica y especializada ya que deben seleccionar, modificar y mantener el complejo software del sistema operativo.

Los especialistas no estarán directamente en la Coordinación de Incidentes Informáticos, se trabajara en coordinación con ellos, cuando ocurran fallas en los programas ya elaborados por el personal de implementación de software especifico, de la Universidad Michoacana de San Nicolás de Hidalgo ubicados en el edifico N.

Sus funciones son:

- Atender todos los incidentes que le sean asignados por la C.I.I. respecto a software específico, ya sea de mantenimiento, actualización o fallas en el mismo.
- Coordinar la presentación de las nuevas aplicaciones a los usuarios.
- Diseñar los planes de calidad de las aplicaciones y garantizar su cumplimiento.
- Validar los nuevos procedimientos y políticas a seguir por las implementaciones de los proyectos liberados.
- Atender todas las fallas técnicas que tengan que ver con la S.I.I.A., educación a distancia, etc. Entre otros tipos de software que ha sido diseñado por ellos.
- Implementar nuevo software y hacer llegar los manuales correspondientes para los usuarios.
- Documentar el reporte de incidente, notificando las acciones que hallan realizado para resolverlo.

El procedimiento se puede apreciar de la siguiente manera en el diagrama de flujo:

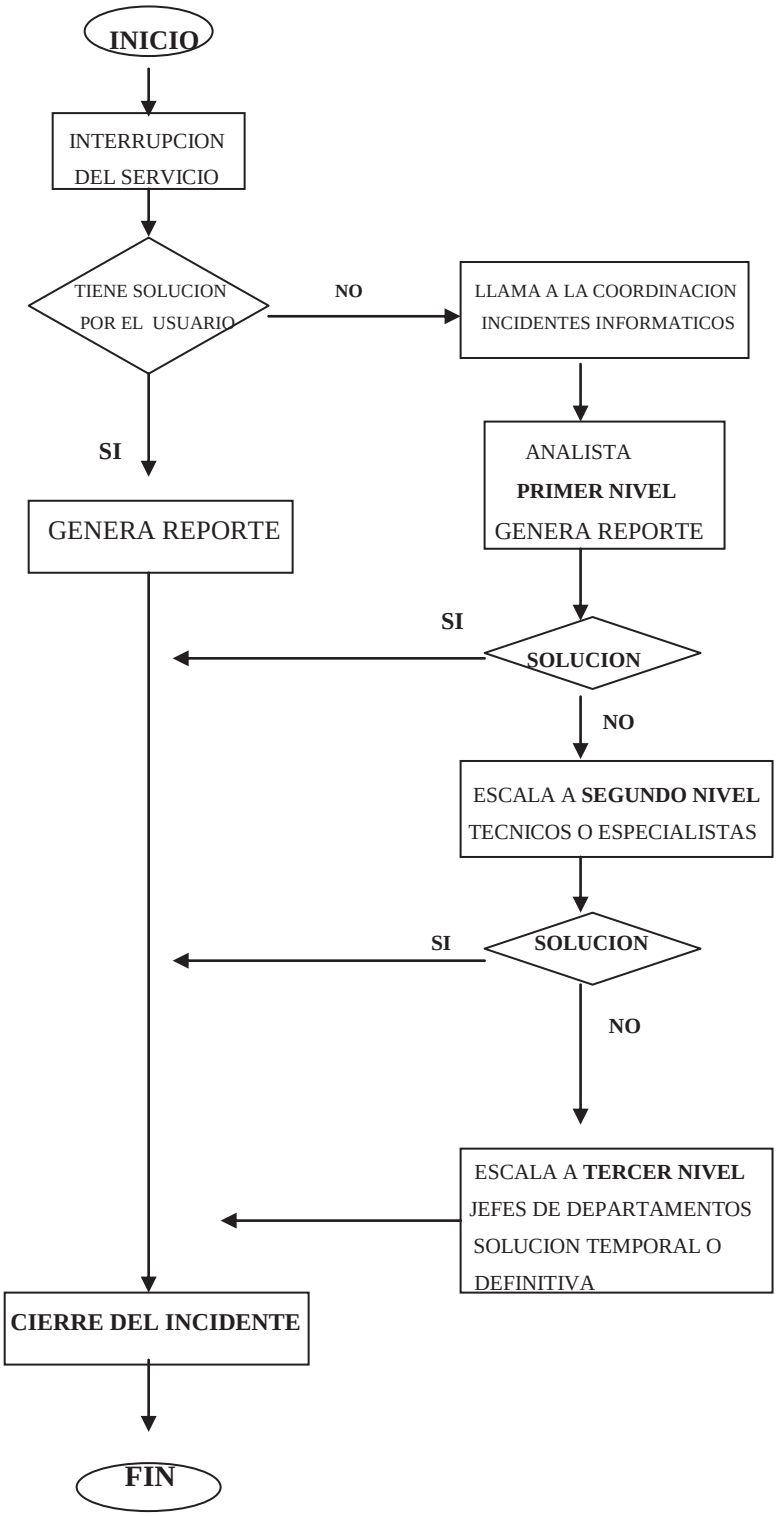


Jefes de departamento: Son las personas encargadas de dirigir, coordinar, supervisar y tomar decisiones en cada departamento de la Facultad de Contaduría Ciencias Administrativas, la Coordinación de Incidentes Informáticos, trabajara en conjunto con lo jefes de departamento, esto con la finalidad de tomar una decisión temporal o definitiva cuando se le presente algún tipo de incidente informático que este deteniendo u obstaculizando la operación de algún departamento.

Las funciones de de los jefes de departamento son:

- Levantar el reporte del incidente informático en la Coordinación de Incidentes Informáticos.
- Una vez que fue escalado por primer y segundo nivel y que no se obtuvo ninguna respuesta satisfactoria, entonces tomaran una decisión definitiva o temporal en conjunto con el administrador de incidentes informáticos.
- Una vez que el incidente halla sido resuelto, deberá comunicarse a la Coordinación de Incidentes Informáticos y autorizar el cierre de incidente satisfactoriamente.

El procedimiento se puede apreciar de la siguiente manera en el diagrama de flujo:



5.0 SEGURIDAD

Seguridad**:** Conjunto de garantías que se da a alguien sobre el cumplimiento de algo. Se dice también de todos aquellos objetos, dispositivos, medidas, etc., que contribuyen a hacer más seguro el funcionamiento o el uso de una cosa.

Así como las computadoras han proporcionado conveniencia, fortaleciendo nuestras economías y transformando al mundo, también han desenterrado nuevos peligros y revelado urgencias. Las estrategias de seguridad se han convertido en un componente esencial de los sistemas de comunicación e información y debemos tener adecuadas normas en materia de intromisiones robo de información digital, fraudes, hacking y amenazas por medio de ellas.

Seguridad informática: Son las técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del hardware, la pérdida física de datos y el acceso a bases de datos por personas no autorizadas. Diversas técnicas sencillas pueden dificultar la delincuencia informática. Por ejemplo, el acceso a información confidencial puede evitarse destruyendo la información impresa, impidiendo que otras personas puedan observar la pantalla del ordenador, manteniendo la información y los ordenadores bajo llave o retirando de las mesas los documentos sensibles. Sin embargo, impedir los delitos informáticos exige también métodos más complejos.

La seguridad informática es un tema muy importante para cualquier institución o empresa, este o no conectada a una red pública. No solamente es importante, sino que también puede llegar a ser compleja. Los niveles de seguridad que se pueden implementar en un centro de cómputo son muchos, y dependerá del administrador para que el usuario logre llegar hasta donde no es necesario que navegue.

La seguridad informática debe cuidar varios aspectos que pueden llegar a ser atacados como:

⇒ Hardware: Este debe ser protegido directamente por los usuarios deben hacer buen uso de el, para lograr obtener una vida útil ganadera, de acuerdo a lo estipulado en los manuales de compra.

⇒ Software: Este puede ser dañado y atacado de manera muy sencilla ocasionando el mal funcionamiento de algún programa, si no es protegido por uno o varios programas denominados antivirus o antispam, es importante que cuidemos que todos los programas de la institución estén protegidos con antivirus actualizados, para poder disponer los programas eficientemente.

⇒ Bases de datos: Estas deben ser protegidas con especial cuidado ya que las bases de datos contienen la información de la institución y esta siempre debe ser integra y libre de cualquier inquilino malicioso, para esto el DBA deberá restringir el acceso a ciertos usuarios. Es importante implementar mecanismos que permitan el control de la consistencia de los datos evitando que estos se vean perjudicados por cambios no autorizados o previstos.

⇒ Redes: Las redes son un canal de comunicación muy importante, el cual debe ser protegido de manera muy detallada y exhaustiva, para que estas no sean monitoreadas o invadidas por intrusos, se deben de tomar ciertas medidas de seguridad, respecto al cableado, debe estar protegido y la estructura de la ubicación debe ser donde no este al acceso de manos maliciosas, para esta área se cuenta con la encriptación y autenticación son herramientas muy importantes que ayudan a proteger la información, en su envió para que solo el emisor y receptor los conozcan.

Ninguna de las anteriores puede tomarse el privilegio de estar en riesgo de algún tipo de vulnerabilidad ya que esto pondría en riesgos a las demás.

5.1 SEGURIDAD DE ACCESO AL SISTEMA.

La información de toda institución o empresa es importante, aunque algunos datos lo son mas que otros, por está razón se debe considerar el control de acceso a los mismos, no todos los usuarios pueden visualizar alguna información, por tal motivo para que un sistema de bases de datos sea confiable debe mantener un grado de seguridad que garantice la autenticación y protección de los datos.

La seguridad en un equipo: Uno de los primeros puntos a cubrir son las claves de acceso a la pantalla de inicio, no se deben usar claves que en su constitución son muy comunes, como es el caso de las iniciales del nombre propio y la fecha de nacimiento, apodos o sobrenombres que todo mundo conoce, o constituirlas de solo letras o solo números; estos tipos de claves son en las que los intrusos y ladrones buscan de primera mano; hay que hacer combinaciones de letras mayúsculas, minúsculas y números alternadamente. No hay que compartir las claves, es común que cuando alguien más necesita usar nuestros equipos, computadoras y sistemas les damos las claves de uso y muchas veces hasta en voz alta, enfrente de muchas personas que no son parte de la empresa las damos a conocer. Hay que cambiar periódicamente las claves de acceso, los equipos o computadoras que se encuentran más expuestos, tienen que tener un cambio más recurrente.

Las conexiones de acceso remoto pueden ser intervenidas para obtener acceso no autorizado hacia las organizaciones y por consiguiente, deben de estar protegidas. Este tipo de conexiones pueden ser por marcación telefónica o atreves de Internet.
Puesto que estas conexiones entran a la red de la empresa o a la computadora tiene que tener un sistema de autentificación como los módems de retroalimentación (que contienen en si mecanismos de autentificación); también existen programas y dispositivos de encriptación para asegurar que la información no sea alterada desde su creación hasta su lectura por el receptor.

En las instituciones y empresas siempre manejan programas y sistemas de acuerdo a las necesidades de estas y para esto deben de contar con métodos de autenticación actuales y que de verdad colaboren a proteger la información de usuarios no deseados, para esto siempre se debe de contar con un administrador de cuentas y privilegios que otorgué los accesos a ciertos usuarios según las necesidades de cada uno.

El DBA (Data Base Administrator) responsable de proveer técnicas que permitan a ciertos usuarios tener acceso a porciones selectas de una base de datos sin tener acceso al resto. Por lo regular un DBA cuenta con un subsistema de seguridad de autorización de la base de datos que se encarga de garantizar la seguridad de porciones de la base de datos contra el acceso no autorizado.

Entre las obligaciones del DBA está otorgar privilegios a los usuarios y clasificar los usuarios y los datos de acuerdo con la política de la institución. Las órdenes privilegiadas del DBA incluyen los siguientes tipos de acciones:

1. Creación de cuentas
2. Concesión de privilegios.
3. Revocación de privilegios.
4. Asignación de niveles de seguridad.

Si los equipos o servidores tienen niveles de permisos de uso de archivos y de recursos, hay que configurarlos de acuerdo a los requerimientos de la empresa o usuario, y no usar la configuración predeterminada que viene de fábrica, así como nombres y usuarios. Los intrusos, ladrones y Hackers conocen muy bien las configuraciones predeterminadas y son las que usan al momento de realizar un ataque.

El objetivo es describir cuales son los métodos más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática (confidencialidad, integridad y disponibilidad de la información) de una institución o empresa, y que armas podemos implementar para la defensa, ya que saber cómo nos pueden atacar y desde donde, es tan importante como saber con que soluciones contamos para prevenir, detectar y reparar un siniestro de este tipo. Sin olvidar que éstas últimas siempre son una combinación de herramientas que tienen que ver con tecnología y recursos humanos políticas, capacitación.

Aspectos fundamentales sobre la información, que la seguridad informática debe cuidar:

⇒ Confidencialidad. No desvelar datos a usuarios no autorizados. Comprende también la privacidad (protección de datos personales).

⇒ Disponibilidad. La información debe estar disponible apropiadamente para cada usuario dependiendo del perfil de esté.

⇒ Integridad. Permite asegurar que los datos no han sido falseados.

Confidencialidad

En un DBA (Data Base Administrator) existen diversos elementos que ayudan a controlar el acceso a los datos. En primer lugar el sistema debe identificar y autenticar a los usuarios utilizando alguno de las siguientes formas:

- Código y contraseña
- Identificación por hardware
- características bioantropométricas (huellas dactilares, voz, retina del ojo)
- Conocimientos, aptitudes y hábitos del usuario
- Información predefinida, el administrador deberá especificar los privilegios que un usuario tiene sobre los objetos:
- Consultar ciertos datos
- Actualizar datos.

Para facilitar la administración los DBA (Data Base Administrator) suelen incorporar el concepto de perfil, rol o grupo de usuarios que agrupa una serie de privilegios por lo que el usuario que se asigna a un grupo hereda todos los privilegios del grupo. El mecanismo de control de acceso se encarga de denegar o conceder el acceso a los usuarios

Disponibilidad

Los sistemas de bases de datos deben asegurar la disponibilidad de los datos a aquellos usuario que tienen derecho a ello por lo que proporcionan mecanismos que permiten recuperar la base de datos contra fallos lógicos o físicos que destruyan los datos en todo o en parte. Aunque sólo nos centraremos en utilidades propias del DBA, sería conveniente además, contar con facilidades ajenas al DBA como, por ejemplo, máquinas tolerantes a fallos, sistemas de alimentación ininterrumpida. El principio básico en el que se apoya la recuperación de la base de datos ante cualquier fallo es la redundancia física.

Integridad

El objetivo en cuanto a la integridad es proteger la base de datos contra operaciones que introduzcan inconsistencias en los datos, por eso hablamos de integridad en el sentido de *corrección*, *validez* o *precisión* de los datos de la base. El subsistema de integridad de un BDA debe, por tanto, detectar y corregir, en la medida de lo posible, las operaciones incorrectas.

La Coordinación de Incidentes Informáticos, entrara en operación con un administrador, dos analistas, dos técnicos y dos especialistas, estos tendrán privilegios de acuerdo al rol de cada uno y los otorgara el administrador de incidentes informáticos, que será el responsable también de otorgar estos privilegios.

El sistema contara con ciertas características muy particulares que cuidaran las medidas de seguridad de la información que manejara el departamento, entre ellas contraseñas para acceder a Windows, contraseña para acceder al sistema de la C.I.I y contraseña para desbloquear por inactividad después de cinco minutos, esto ayudara a tener cierto control en diferentes plataformas de los equipos y protegerá la información de intrusos.

5.2 SEGURIDAD SOBRE LAS INSTALACIONES.

El objetivo es describir cuales son los métodos más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática (confidencialidad, integridad y disponibilidad de la información) de una institución o empresa, y que armas podemos implementar para la defensa, ya que saber cómo nos pueden atacar y desde donde, es tan importante como saber con que soluciones contamos para prevenir, detectar y reparar un siniestro de este tipo. Sin olvidar que éstas últimas siempre son una combinación de herramientas que tienen que ver con tecnología y recursos humanos políticas, capacitación, etc.

La seguridad física debe ser empleada junto con la seguridad administrativa y técnica para brindar una protección completa. Ninguna cantidad de seguridad técnica puede proteger la información confidencial si no se controla el acceso físico a los servidores, equipos y computadoras. Igualmente, las condiciones climáticas y de suministro de energía pueden afectar la disponibilidad de los sistemas de información.

El acceso físico es importante, todos los equipos delicados deben de estar protegidos del acceso no autorizado; normalmente esto se consigue concentrando los sistemas en un centro de datos. Este centro esta controlado de diferentes maneras, se puede limitar el acceso con dispositivos, o instalar cerraduras de combinación para restringir los accesos a empleados y personas ajenas a las instalaciones.

Los sistemas de cómputo son sensibles a las altas temperaturas. Los equipos de cómputo también generan cantidades significativas de calor. Las unidades de control de clima para los centros de cómputo o de datos deben de ser capaces de mantener una temperatura y humedad constante.

Los sistemas de extinción de incendios para los equipos deben ser los apropiados, estos no tienen que tener base de agua para que no dañen los equipos.
Para evitar pérdidas y daños físicos a equipos y computadoras hay que contar con una instalación eléctrica adecuada, no hay que saturar tomas de corriente, se recomienda utilizar fuentes reguladas como no-breaks y reguladores para la protección de equipos. Si existen instalaciones específicas para los equipos y computadoras se recomienda utilizar fuentes redundantes y una planta de energía auxiliar.

La seguridad física, como la ubicación de los centros de procesos, las protecciones físicas, el control físico de accesos, los vigilantes, las medidas contra el fuego y el agua, y otras similares.

Cifrado de datos: Sirve para proteger datos confidenciales que se transmiten por satélite o algún tipo de red de comunicaciones. Asimismo el cifrado puede proveer protección adicional a secciones confidenciales de una base de datos. Los datos se codifican mediante algún algoritmo de codificación. Un usuario no autorizado tendrá problemas para descifrar los datos codificados, pero un usuario autorizado contará con algoritmos para descifrarlos.

Seguridad técnica, se ocupan de la implementación de los controles de seguridad sobre los sistemas de cómputo y de red. Estos controles son manifestaciones de las políticas y los procedimientos de la organización.

En las empresas como en las casas ya se cuenta con conexiones permanentes a las redes o a Internet y estas deben de estar protegidas mediante muros de fuego que actúan de manera que su homónimo arquitectónico entre dos habitaciones de un edificio. Puede ser físico (equipo) ó lógico (software).

Uno de los objetivos de la seguridad informática es librar la información de riesgos, amenazas o vulnerabilidades.

Amenazas

Evento no deseado que puede afectar los intereses de una organización. Las amenazas ambientales incluyen a los desastres naturales y otras condiciones ambientales. Un desastre natural puede ocasionar perdida de disponibilidad y al combinarlo con seguridad física pobre obtenemos perdida de confidencialidad.

Estos pueden ser, errores de programación, errores de configuración, ausencia de personal responsable, fallas técnicas, hardware, Falta de corriente, Interferencias eléctricas, Daños físicos, software de aplicación, Alteración de programas, Robos de programas, Fallos de los mecanismos de seguridad, Redes de comunicación, Ruptura de conexiones, Problemas con el cableado, etc.

Riesgos

Probabilidad de que una amenaza se vuelva real, proximidad o posibilidad de un daño, peligro, etc. Limitándonos a la seguridad propiamente dicha, los riesgos pueden ser múltiples: el primer paso es conocerlos, y el segundo es tomar decisiones al respecto; el conocerlos y no tomar decisiones no tiene sentido y debiera crearnos una situación de desasosiego.

Como las medidas tienen un coste, a veces los directivos se preguntan a los consultares, cuál es el riesgo máximo que podría soportar su entidad, si bien la respuesta no es fácil, porque dependen de la criticidad del sector y de la entidad misma, de su dependencia respecto a la información, y del impacto que su disponibilidad pudiera tener en la entidad. Si nos basamos en el impacto nunca debería aceptarse un riesgo que pudiera llegar a poner en peligro la propia continuidad de la entidad, pero este listón es demasiado alto.

Por debajo de ello hay daños de menores consecuencias, siendo los errores y omisiones la causa más frecuente, normalmente de poco impacto pero frecuencia muy alta, y otras el acceso indebido a los datos a veces a través de redes, la sesión no autorizada de soportes magnéticos con la información sensible, los daños por fuego, por agua del exterior como puede ser una inundación, o una tubería interior, la variación no autorizada de programas, persiguiendo el propio beneficio o el causar un daño, a veces por venganza.

Vulnerabilidades

Vulnerabilidad. Una característica que puede ser utilizada por una amenaza.

Ejemplos de vulnerabilidades para amenazas accidentales:

Falta de capacitación al personal.

Falta de procedimientos.

Falta de redundancia en equipos.

Falta de respaldo de información.

Los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red.

Tipos de ataques

Ataques de intromisión: Este tipo de ataque es cuando alguien abre archivos, uno tras otro, en nuestra computadora hasta encontrar algo que le sea de su interés. Puede ser alguien externo o inclusive alguien que convive todos los días con nosotros. Cabe mencionar que muchos de los ataque registrados a nivel mundial, se dan internamente dentro de la organización y/o empresa.

Ataque de espionaje en líneas: Se da cuando alguien escucha la conversación y en la cual, él no es un invitado. Este tipo de ataque, es muy común en las redes inalámbricas y no se requiere, como ya lo sabemos, de un dispositivo físico conectado a algún cable que entre o salga del edificio. Basta con estar en un rango donde la señal de la red inalámbrica llegue, a bordo de un automóvil o en un edificio cercano, para que alguien esté espiando nuestro flujo de información.

Ataque de intercepción: Este tipo de ataque se dedica a desviar la información a otro punto que no sea la del destinatario, y así poder revisar archivos, información y contenidos de cualquier flujo en una red.

Ataque de modificación: Este tipo de ataque se dedica a alterar la información que se encuentra, de alguna forma ya validada, en computadoras y bases de datos. Es muy común este tipo de ataque en bancos y casas de bolsa. Principalmente los intrusos se dedican a cambiar, insertar, o eliminar información y/o archivos, utilizando la vulnerabilidad del los sistemas operativos y sistemas de seguridad (atributos, claves de accesos, etc.).

Ataque de denegación de servicio: Son ataques que se dedican a negarles el uso de los recursos a los usuarios legítimos del sistema, de la información o inclusive de algunas capacidades del sistema. Cuando se trata de la información, esta, se es escondida, destruida o ilegible. Respecto a las aplicaciones, no se pueden usar los sistemas que llevan el control de la empresa, deteniendo su administración o inclusive su producción, causando demoras y posiblemente pérdidas millonarias. Cuando es a los sistemas, los dos descritos anteriormente son inutilizados. Si hablamos de comunicaciones, se puede inutilizar dispositivos de comunicación (tan sencillo como cortar un simple cable), como saturar e inundar con tráfico excesivo las redes para que estas colisionen.

Ataque de suplantación: Este tipo de ataque se dedica a dar información falsa, a negar una transacción y/o a hacerse pasar por un usuario conocido. Se ha puesto de moda este tipo de ataques; los "nuevos ladrones" ha hecho portales similares a los bancarios, donde las personas han descargado sus datos de tarjetas de crédito sin encontrar respuesta; posteriormente sus tarjetas de crédito son vaciadas.

Es importante mencionar, que así como se llevan estos tipos de ataques en medios electrónicos, muchas veces se llevan a cabo en archivos físicos (expedientes, archiveros con información en papel, y en otro tipo de medios con los que las personas están familiarizadas a trabajar todos los días (como teléfonos convencionales, celulares, cajeros automáticos, etc.); inclusive los ataques a computadoras, muchas veces, comienzan precisamente con información obtenida de una fuente física (papeles, basura, intervención de correo, cartas, estados de cuenta que llegan a los domicilios; o simplemente de alguien que vigila lo que hacemos).

La intrusión, pérdida, alteración, inserción, bloqueo de información en sistemas, bloqueo de sistemas operativos y de dispositivos, suceden por casualidad o simplemente por que existen los Hackers.

Para proteger los posibles ataques que pudiera llegar a sufrir las instalaciones de La Coordinación de Incidentes Informáticos, se deben de implantar ciertas medidas que protejan las redes, la comunicación, las instalaciones físicas y el software de operación y para esto podemos disponer de las siguientes herramientas:

a) Un firewall o combinación de ellos.
b) Proxies.
c) Un sistema de detección de intrusos o IDS.
d) Sistemas de actualización automática de software.
e) Sistemas de control de la integridad de los servidores, paquetes, etc.
f) Un sistema de administración y control para monitorear la seguridad.
g) Un cableado protegido para evitar vulnerabilidades por medio de la red.

Firewall

Es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. Es un mecanismo para restringir acceso entre la Internet y la red corporativa interna. Típicamente se instala un firewall en un punto estratégico donde una red (o redes) se conectan a la Internet.

Un buen Firewall para Internet puede ayudarle a impedir que extraños accedan a su PC desde Internet. Los Firewalls pueden ser de dos tipos, de software o de hardware, y proporcionan una frontera de protección que ayuda a mantener fuera a los invasores no deseados de Internet.

La existencia de un firewall en un sitio Internet reduce considerablemente las probabilidades de ataques externos a los sistemas corporativos y redes internas, además puede servir para evitar que los propios usuarios internos comprometan la seguridad de la red al enviar información peligrosa (como passwords no encriptados o datos sensitivos para la organización) hacia el mundo externo.

Si el Firewall "observa" alguna actividad sospechosa: que alguien de fuera esté intentando acceder a nuestro Pc o que algún programa espía trate de enviar información sin consentimiento, el Firewall nos advertirá con una alarma en el sistema.

Un firewall sirve para múltiples propósitos, entre otros podemos anotar los siguientes:

- Restricción de entrada de usuarios a puntos cuidadosamente controlados de la red interna.
- Prevención ante los intrusos que tratan de ganar espacio hacia el interior de la red y los otros esquemas de defensas establecidos.
- Restricción de uso de servicios tanto a usuarios internos como externos.
- Determinar cuáles de los servicios de red pueden ser accesados dentro de ésta por los que están fuera, es decir, quién puede entrar a utilizar los recursos de red pertenecientes a la organización.

Todo el tráfico que viene de la Internet o sale de la red corporativa interna pasa por el firewall de tal forma que él decide si es aceptable o no.

Sistemas de actualización automática de software.

En computadoras que utilicen sistemas operativos de Microsoft, hay que realizar actualizaciones periódicamente, ya que constantemente los Hacker y creadores de virus encuentran vulnerabilidades en dichos sistemas operativos.

En cada nodo y servidor hay que usar antivirus, actualizarlo o configurarlo para que automáticamente integre las nuevas actualizaciones del propio software y de las definiciones o bases de datos de virus registrados.

Un sistema de administración y control para monitorear la seguridad.

También, hay que utilizar programas que detecten y remuevan "spywares" (programas o aplicaciones que recopilan información sobre una persona u organización sin su conocimiento), existen diferente software que realizan esta tarea, algunos son gratuitos y trabajan muy bien; así la recomendación es contar con uno de ellos y realizar un escaneo periódico de el equipo o computadora.

5.3 SEGURIDAD SOBRE EL MANEJO Y ADMINISTRACIÓN DE LA INFORMACIÓN.

La seguridad administrativa, esta basada en políticas y normas que se deben de implantar y seguir. Las políticas que proporcionan las reglas que gobiernan el cómo deberían ser configurados los sistemas y cómo deberían actuar los empleados de una organización en circunstancias normales y cómo deberían reaccionar si se presentan circunstancias inusuales. Define lo que debería de ser la seguridad dentro de la organización y pone a todos en la misma situación, de modo que todo el mundo entienda lo que se espera de ellos.

El manejo y administración de la información no puede estar en manos de cualquier persona, esta debe ser cuidada de manera especial, y el administrador de la Coordinación de Incidentes Informáticos, debe controlar gradualmente los permisos y accesos a la información. Los sistemas de bases de datos contienen grandes cantidades de información, la manipulación de los datos, involucra tanto la definición de estructuras para el almacenamiento de la información como la provisión de mecanismos para la manipulación de la información, esto debe anteponer criterios de seguridad, que garanticen la integridad de la información, a pesar de las caídas del sistema o intentos de accesos no autorizados.

Autenticación, que no es otra cosa más que el mecanismo necesario para asegurarse de que el usuario es realmente quien dice ser.

Encriptación: Consiste en codificar de forma en que solo el remitente y el destinatario puedan entenderlos. Esta basado en el uso de claves para descifrar mensajes con reglas previamente establecidas.

Auditorias: Es un método donde el sistema es capaz de notificar al administrador, sobre cualquier anomalía o evento importante.

La información de la Coordinación de Incidentes Informáticos, será totalmente confidencial, únicamente hará uso de ella personal autorizado como lo son los analistas, especialistas y el administrador de la Coordinación, esto con la finalidad de mantener seguridad en las posibles debilidades que pudiera llegar a presentar la Facultad de Contaduría Ciencias Administrativas en cuanto al servicio informático.

6.0 NORMAS GENERALES

Las normas, estudian la organización y funcionamiento de un lugar, consiste en dirigir el comportamiento de las personas que realizan diferente tipos de acciones. Las políticas y reglas están relacionadas con la administración que llevan en las instituciones, se relacionan con la autoridad y tienen por objeto establecer medidas que controlen a personas para obtener ciertos resultados sobre determinado lugar.

Las políticas son consideradas como un conjunto de ideas, creencias, usos y practicas sociales, relacionadas con la administración y la autoridad, consiste en el buen modo de comportarse, las políticas establecidas en cualquier institución, empresa, región o estado, son un medio que se emplea para conseguir ciertos fines.

Las reglas marcan los márgenes a los que estarán sujetas ciertas personas al prescindir de un servicio o de un lugar, para de esta forma tener un control interno sobre los estándares de cierto lugar y así protegerlo de malas actitudes de los usuarios.

En la presente tesis se establecerán ciertas políticas y reglas, con la finalidad de tener cierto control sobre las acciones que se puedan llegar a desenvolver respecto al uso de los equipos de computo de la Facultad de Contaduría Ciencias Administrativas, esto para evitar el mal uso del hardware, software y sistemas, para que los usuarios tengan ciertas limitantes, y evitar acciones que afecten a la institución ocasionándole perdidas tanto físicas, económicas, etc.

6.1 POLITICAS DE LA F.C.C.A. EN CUANTO SOFTWARE Y HARDWARE

- Toda la Institución podrá utilizar únicamente el hardware y el software que sea otorgado por la Coordinación de Incidentes Informáticos, le haya instalado y oficializado mediante el "Acta de entrega de equipos y/o software".

- Tanto el hardware y software, como los datos, son propiedad de la Facultad de Contaduría Ciencias Administrativas, su copia o sustracción o daño intencional o utilización para fines distintos a las labores propias de la compañía, será sancionada de acuerdo con las normas ya establecidas.

- La Coordinación de Incidentes Informáticos, llevara el control del hardware y el software instalado, basándose en el número de serie que contiene cada uno.

- Periódicamente, la Coordinación de Incidentes Informáticos en colaboración con sus técnicos, efectuará visitas para verificar el software utilizado en cada computadora de la Facultad de Contaduría Ciencias Administrativas. Por lo tanto, el detectar software no instalado por la Coordinación de Incidentes Informáticos, será considerado como una violación.

- Toda necesidad de hardware y/o software adicional debe ser solicitada por escrito al la Coordinación de Incidentes Informáticos, quien justificará o no dicho requerimiento, mediante un estudio evaluativo.

- La Coordinación de Incidentes Informáticos, instalará el software en cada computador y entregará al área usuaria los manuales pertinentes los cuales quedaran bajo la responsabilidad del Jefe del departamento respectivo.

- Los Cd´s que contienen el software original de cada paquete serán administrados y almacenados por el La Coordinación de Incidentes Informáticos.

- La Coordinación de Incidentes Informáticos, proveerá al personal docente académico o estudiantil el software en caso de requerirse la reinstalación de un paquete determinado.

- Los trámites para la compra de los equipos aprobados por la Coordinación de Incidentes Informáticos, así como la adecuación física de las instalaciones serán realizadas por medio de una respectiva licitación.

- La prueba, instalación y puesta en marcha de los equipos y/o dispositivos, serán realizada por la Coordinación de Incidentes Informáticos, quien una vez compruebe el correcto funcionamiento, oficializara su entrega al área respectiva mediante el "Acta de Entrega de Equipos y/o Software".

- Una vez entregados los equipos de computación y/o el software por la Coordinación de Incidentes Informáticos, estos serán cargados a la cuenta de activos fijos del área respectiva y por lo tanto, quedaran bajo su responsabilidad.

- Así mismo, la Coordinación de Incidentes Informáticos mantendrá actualizada la relación de los equipos de computo de la institución, en cuanto a numero de serie y ubicación, con el fin que este mismo departamento verifique, por lo menos una vez al año su correcta destinación y ubicación.

- La Coordinación de Incidentes Informáticos, actualizará el software comprado cada vez que una nueva versión salga al mercado, a fin de aprovechar las mejoras realizadas a los programas, siempre y cuando se justifique esta actualización.

6.2 REGLAS DE LA COORDINACION DE INCIDENTES INFORMATICOS

Las reglas en cualquier institución o empresa marcan la línea que debe perseguir esto con la finalidad de tener cierto orden y control sobre las actividades que se realizan en determinado departamento, área u oficina, las reglas son el apoyo de cualquier departamento ya que en base a esto realizan sus actividades diarias.

Las reglas nos ayudan en la Coordinación de Incidentes Informáticos a elevar la calidad y cantidad de los servicios que ofrece dicha Coordinación, a todos sus usuarios que demandan simplificación y eficiencia al máximo para la atención de sus necesidades, todo ello en el marco de la cooperación y la responsabilidad del personal que lo integra, además de continuar sensibilizando a Directivos, Alumnado, Personal Docente y Administrativo, sobre las ventajas de hacer uso de las nuevas tecnologías como un apoyo de gran valor en su labor diaria, pero para lograr esto sin duda, deben existir ciertas reglas que rijan a la Coordinación de Incidentes Informáticos y a sus usuarios.

REGLAMENTO PARA USUARIOS DE LA COORDINACION DE INCIDENTES INFORMATICOS

- El horario de atención a los usuarios es de 8:00 a 20:00 hrs. de lunes a viernes y los sábados de 9:00 a 14:00 hrs.

- Al levantar un reporte sobre algún incidente el usuario deberá identificarse con credencial de la Universidad Michoacana de San Nicolás de Hidalgo o bien con su matricula, en caso de ser docente o personal administrativo deberá ser su numero de empleado cualquiera de estos dos, tendrá que ser vigente, de no ser así, no estará autorizado para utilizar el servicio informático y mucho menos para levantar reportes.

- El servicio de consulta vía Internet estará sujeto al acceso a temas con carácter educativo o de investigación; otros temas pudieran tener restricciones. (El uso prolongado de correo electrónico, el manejo de chat, mensajeros instantáneos y otros están restringidos).

- No fumar en las Instalaciones de los laboratorios.

- Cualquier usuario que no acate las disposiciones establecidas en el presente reglamento o sea sorprendido dañando o sustrayendo material o equipo propiedad de los laboratorios, será suspendido de la prestación del servicio y turnado a las autoridades correspondientes. La suspensión prevalecerá hasta en tanto no sea resuelta la situación del usuario.

- No introducir ninguna clase de alimento o bebida a los Laboratorios.

- El usuario es responsable del equipo que se le haya asignado, por lo que se recomienda verificar las condiciones en que se recibe y reportar cualquier anomalía al encargado, dado que los gastos de reparación por daño causado al equipo y/o mobiliario serán cubiertos por el usuario responsable.

- No está permitido utilizar el equipo con juegos de video, dadas las características de los laboratorios como área exclusiva de trabajo.

- Se prohíbe la instalación de cualquier tipo de programas sin la autorización de la Coordinación de Incidentes Informáticos, (las enciclopedias y programas educativos pueden ser instalados en un área especial y se desinstalaran a la brevedad posible).

- El usuario podrá guardar archivos personales en el disco duro de la máquina que emplea, pero debe saber que la dicha información es borrada en los períodos vacacionales por cuestiones de mantenimiento.

- No está permitido cambiar la ubicación del equipo.

- El usuario (s) podrá ser suspendido en su derecho de utilizar los servicios de los laboratorios en caso de infracción grave al presente reglamento.

REGLAMENTO PARA EL PERSONAL DE LA COORDINACION DE INCIDENTES INFORMATICOS

- Queda estrictamente prohibido la usurpación de actividades o trabajos de sus propios compañeros ya que deberá cubrir cada quien su puesto en un 100% con la finalidad de no descuidar sus actividades ya establecidas por realizar las de algún otro compañero.

- No introducir ninguna clase de alimento o bebida a la Coordinación de Incidentes Informáticos.

- No fumar en las Instalaciones de la Coordinación de Incidentes Informáticos.

- El usuario es responsable del equipo que se le haya asignado, por lo que se recomienda verificar las condiciones en que se recibe y reportar cualquier anomalía al encargado, dado que los gastos de reparación por daño causado al equipo y/o mobiliario serán cubiertos por el usuario responsable.

- No está permitido cambiar la ubicación del equipo.

- No está permitido utilizar el equipo con juegos de video, dadas las características de la Coordinación de Incidentes Informáticos, es como área exclusiva de trabajo.

- Se prohíbe la instalación de cualquier tipo de programas sin la autorización del administrador de incidentes.

- El personal de la Coordinación de Incidentes Informáticos, deberá apagar el equipo de acuerdo con las indicaciones generales o bien solicitar ayuda al encargado cuando así lo requiera, deberá además dejar en orden el mobiliario y equipo utilizado.

- Cualquier usuario que no acate las disposiciones establecidas en el presente reglamento o sea sorprendido dañando o sustrayendo material o equipo propiedad del centro de Cómputo será suspendido de la prestación del servicio y turnado a las autoridades correspondientes. La suspensión prevalecerá hasta en tanto no sea resuelta la situación del usuario.

- El uso sonido (escuchar discos de música, programas multimedia y otros) será permitido siempre y cuando el usuario utilice audífonos.

- Cualquier aspecto no considerado dentro de este reglamento será sujeto de revisión y acuerdo por parte de los responsables del Centro y /o Autoridades correspondientes

- El usuario (s) podrá ser suspendido en su derecho de utilizar los servicios de los laboratorios en caso de infracción grave al presente reglamento.

6.3 PROCEDIMIENTOS

Los procedimientos de un área o departamento, son los pasos por los que tiene que pasar cierta tarea que se realiza en dicho lugar, la Coordinación de Incidentes Informáticos cuenta con ciertos procedimientos que ya hemos mencionado anteriormente pero en este capitulo los señalaremos con mas detalles.

Como ya hemos mencionado la Coordinación de Incidentes Informáticos, tiene como finalidad dar una solución a corto tiempo a todos los incidentes informáticos, que sucedan en la Facultad de Contaduría Ciencias Administrativas, y para que esto suceda debe existir un procedimiento y un tiempo de respuesta en cada uno de los pasos o escalas por las que pase un incidente.

Los procedimientos que realiza la Coordinación de Incidentes Informáticos, buscan el cumplimiento satisfactorio de los servicios informáticos, y mantener tantos el hardware como software y sistema, disponible para los usuarios.

El procedimiento que aplica la Coordinación de Incidentes Informáticos es el siguiente:

Primer Nivel

Analistas

Procedimiento de administración de incidentes

Aquí se identifica al usuario, de donde llama, datos personales de empleado o estudiante, posteriormente con que elementos esta conectado o tiene relación y si los elementos en uso están autorizados, una vez analizado esto, se apoyara en la gestión de la manera correspondiente, para que a este nivel se pueda resolver el incidente del usuario, de no de ser así será escaldo a segundo nivel.

De acuerdo al procedimiento, este nivel deberá atender todos los incidentes de solución en línea, errores técnicos de bajo nivel o correspondiente a las facultades con las que cuenta el DBA administrador de la base de datos de usuarios, como son:

- Bloqueos de contraseñas
- Creación de cuentas de nuevas.
- Privilegios a usuarios.
- Pc´s desconectadas.
- Papel atascado en la impresora.
- Reporte de robo u extravió de alguna pieza de computo.
- Asesoría sobre alguna herramienta de determinado programa, etc.

Segundo Nivel

Especialistas

Procedimiento de administración de la capacidad.

Una vez que fue analizado el incidente que acaba de reportar el usuario, si no fue resuelto en el primer nivel pasa al segundo nivel donde se canaliza con un especialista en el área el cual cuenta con la capacidad para resolverlo, aun siendo así existe la posibilidad de que por algún motivo, razón o circunstancia no se de una solución, motivo por el cual tendrá que ser escalado a tercer nivel.

Este nivel deberá resolver todos los incidentes que tengan que ver con:

- Instalación de software.
- Daño y reemplazo de alguna pieza de hardware.
- Mantenimiento preventivo y correctivo de software y hardware.
- Configuración de programas.
- Mantenimiento a los sistemas oficiales de la FCCA.
- Fallas con el Internet.
- Fallas en con la corriente eléctrica, etc.

Tercer Nivel

Jefes toma de decisiones

Procedimiento de administración de problemas

Cuando el incidente en primer nivel se analizo y no tuvo una pronta respuesta satisfactoria, pasa con el especialista a segundo nivel y si persiste de igual forma sin ser resuelto, pasa a convertirse de incidente a problema y alcanza su último nivel de escalamiento, una vez atendido por el *"Procedimiento de Administración de Problemas"* este regresa ya con una solución definitiva o temporal.

Este nivel deberá resolver todos los incidentes que por algún motivo, no fue posible su pronta solución, aquí el administrador de incidentes informáticos deberá tomar la pauta de tener una muy estrecha relación con el jefe de departamento donde ocurre el incidente, para que entre los dos tomen una decisión considerando sea la mas apropiada, para solucionar el incidente ya sea con una solución temporal o un cambio definitivo en el departamento.

TABLA DE TIEMPOS DE RESOLUCION DE INCIDENTES

ESCALAS	RESPONSABLE	TIEMPO DE RESPUESTA
Primer Nivel	Analista	5 a 10 min.
Segundo Nivel	Especialista	10 a 30 min.
Tercer Nivel	Jefes de departamento	30 a 60 min.

La tabla anterior muestra un estándar de calidad que debe aplicar la Coordinación de Incidentes Informáticos, para cubrir con los objetivos que debe cumplir, aplicando estos tiempos, se obliga a contar con la activa presencia de los servicios informáticos, para que estos permitan realizar tanto al alumnado como al docente académico y administrativo, de la Faculta de Contaduría y Ciencias Administrativas sus actividades laborales y estudiantiles de manera satisfactoria.

7. GUARDA Y CUSTODIA DE DOCUMENTOS

La información es un activo que las instituciones y empresas cuidan con especial cuidado ya que está, ayuda constantemente a la toma de dediciones oportunas y adecuadas para lograr obtener las metas y objetivos que tiene cada departamento, por esta razón la información debe ser protegida y resguardada bajo ciertos criterios de seguridad con la finalidad de que al momento de sufrir un siniestro la institución o empresa, y llegara a tener una perdida total de la información que tiene tanto en documentos como en equipo de computo, la empresa no se vea afectada y logre recuperar la información que tiene protegida y resguardada en otro lugar.

7.1 RESPONSABLES

La información es uno de los activos más importantes de las entidades, y de modo especial en algunos sectores de actividad.

Es indudable que cada día las entidades dependen de mayor medida de la información y de la tecnología, y que los sistemas de información están más soportadas por la tecnología, frente a la realidad de hace pocas décadas.

La Coordinación de Incidentes Informáticos, será un departamento que concentre mucha información sobre los incidentes, acciones, soluciones y administración total de recursos informáticos y equipos de computo, de la Facultad de Contaduría Ciencias Administrativas, toda esta información representa mucha importancia y validez para la facultad y dicho departamento, ya que esto será su razón de ser, por tal motivo la información deberá ser respaldada y resguardada bajo ciertos niveles de seguridad con la finalidad de salvaguardar la información de cualquier siniestro que se pudiera suscitar en cualquier momento.

Por tal motivo se destinara a un grupo de personas dentro de la Facultad para que realicen la labor de respaldos y administración de resguardos de documentación, y de esta manera proteger la información.

Personas responsables:

- Administrador de incidentes informáticos
- Analistas
- Secretario administrativo

7.2 ADMINISTRACIÓN DE DOCUMENTOS

La administración de documentos es una parte muy importante ya que el orden es la base de de cualquier tipo de tarea, el orden es esencial en cualquier departamento que funcione eficientemente y sobre todo si nos referimos a la información, que en cualquier momento podemos llegar a necesitar, esta debe de estar siempre en el lugar adecuado y libre de sufrir algún daño o desperfecto, para esto es importante contar con un proceso de administración de documentos y archivos respaldados, para lograr disponer de ellos en todo momento y bajo cualquier circunstancia o tiempo determinado.

Objetivos del resguardo de documentos y archivos de información son:

- ⇒ Proteger la información de cualquier persona ajena y pudiera llegar hacer mal uso de ella.
- ⇒ Proteger la información de cualquier tipo de siniestro provocado por la naturaleza.
- ⇒ Proteger la información de alguna descarga eléctrica que llegara a dañar los equipos de cómputo y se perdiera la información.
- ⇒ Proteger la información y llevar cierto control y orden mensualmente de esta.
- ⇒ Seguir los controles de estandarización de seguridad de la información para lograr mantener la Confidencialidad, Integridad y Disponibilidad de está.
- ⇒ Librar la información de riesgos, amenazas o vulnerabilidades.
- ⇒ Contar la información, en caso de robo o fraude a la institución.

El proceso de administración de información tanto de documentos como respaldos en CD o cualquier otro medio extraíble, deberá de resguardarse mensualmente primero por los analistas y después revisado y autorizado para su resguardo por el administrador de incidentes informáticos, una vez hecho esto el Administrador deberá hacer llegar la documentación y respaldos de información en CD o disco duros, al secretario administrativo de la facultad, para que este lleve estos documentos y respaldos un lugar externo a la facultad, donde deberá estar la información a salvo de cualquier siniestro o deterioro, esta información estará disponible únicamente para el administrador de incidentes informáticos y directivos de la facultad y en caso de requerir la información resguardada se deberá pedir mediante una solicitud hacia el secretario administrativo, que será el responsable de la disponibilidad de esta información resguardada.

La información la deberá concentrar el administrador de incidentes informáticos, con la ayuda y colaboración de sus subordinados de la siguiente manera:

⇒ Realizar las copias de respaldo (back-up) de la información y procesos de cómputo que se realizan en La Coordinación de Incidentes Informáticos, conforme a parámetros preestablecidos.
⇒ Marcar y/o señalizar los productos de los procesos ejecutados.
⇒ Llevar registros de fallas, problemas, soluciones, acciones desarrolladas, respaldos, recuperaciones y trabajos realizados.
⇒ Cumplir con las normas, reglamentos y procedimientos establecidos por la Dirección para el desarrollo de las funciones asignadas.
⇒ También documentan las actividades diarias, los suministros empleados y cualquier condición anormal que se presente.

Toda esta información explica la operación de la Coordinación de Incidentes Informáticos, y puede llegar a ser solicitada en caso de auditoria u otra situación necesaria.

CONCLUSIONES

La presente tesis, es una clara evidencia sobre la importancia de la administración informática, ya que en la actualidad no existe una empresa exitosa que no administre sus activos de una manera exhaustiva, esto con la finalidad de obtener eficiencia y optimización en sus procesos y recursos, para de esta forma lograr tener mayores utilidades.

El presente proyecto demuestra como la administración de los servicios informáticos no es un gusto, si no una necesidad, por que en el momento que se comienza a administrar estos activos, se esta optimizando recurso computacional que una vez analizado y plasmado en cifras numéricas se podrá apreciar el gran ahorro económico que se esta obteniendo.

Es importante que en toda institución o empresa que tenga una operación constante de sus servicios informáticos, cuente con un centro de apoyo que asesore al usuario sobre las particularidades de los servicios informáticos, y de esta forma administrarlos a la vez, manteniendo así una comunicación constante y productiva con el usuario.

Únicamente teniendo una estrecha comunicación con el usuario y un absoluto control sobre todo el activo computacional, se podrá obtener un buen funcionamiento y aprovechamiento del recurso computacional y el usuario sentirá cierta responsabilidad por los equipos de computo que utilice ya que el monitoreo computacional será una actividad constante que realizara La Coordinación de Incidentes Informáticos.

Durante todo este análisis, el presente proyecto intentaba contestar algunas interrogantes una de ellas era si la Coordinación de Incidentes Informáticos, seria un gasto o una inversión, y la respuesta a esta interrogante es la siguiente…

La Coordinación de Incidentes Informáticos, es una inversión y no un gasto ya que se esta invirtiendo a mediano plazo para que la administración de los servicios informáticos de la Facultad de Contaduría Ciencias Administrativas logren obtener la máxima eficiencia y así ahorrar tiempos, recursos económicos y materiales.

Otra interrogante era:
¿Para que crear la Coordinación de Incidentes Informáticos?, para comenzar a administrar todo el recurso informático de la Facultad de Contaduría Ciencias Administrativas una vez que el usuario cuente con un centro de apoyo de los servicios informáticos, el usuario no sentirá molestia, enojo o desesperación y mucho menos se estará desorientado de no saber que hacer ante la falta del servicio informático, ya que podar contar con la Coordinación de Incidentes Informáticos, que le apoyara a resolver sus incidentes informáticos dentro de la Facultad, entonces una vez que el usuario cuenta con este centro de atención a usuarios de los servicios informáticos, al momento en que se le presente un incidente, únicamente lo tomara con calma y acudirá directamente a comunicarse a la Coordinación de Incidentes Informáticos, para que le asesoren, apoyen y resuelvan sus incidente que le interrumpió sus actividades y una vez resuelto este, continuara desarrollando sus labores.

Una vez analizado todo lo anterior, se demuestra la importancia de la administración informática, y el por que ya no se debe seguir ignorando este suceso tan repetitivo en las instituciones y empresas.

Los costes que originen llevar una administración en una empresa o Institución, nunca será un gasto, siempre será una inversión cuando esta se haga correctamente.

GLOSARIO

Administrador de incidentes: Se refiere a la persona responsable de administrar todo el procedimiento de La Coordinación de Incidentes Informáticos, en colaboración de sus subordinados.

Administración: Proceso de crear, diseñar y mantener un ambiente en el que las personas al laborar o trabajar en grupos, alcancen con eficiencia metas seleccionadas. Las personas realizan funciones administrativas de planeación, organización, integración de personal, dirección y control.

Administración Informática: La administración informática se refiere a la optimización de recursos informáticos en base a la administración correcta de estos.

Analista: El analista tiene como cometido analizar un problema y describirlo con el propósito de ser solucionado mediante un sistema informático.

Las cualidades que se esperan de un analista son esencialmente la capacidad de abstracción y de análisis.

Controlar: Es vigilar para que todo suceda conforme a las reglas establecidas y a las órdenes dadas.

Coordinar: Es ligar, unir y armonizar todos los actos y todos los esfuerzos.

Coordinación Administrativa: Es el área de gestión donde se lleva a cabo el enlace con los departamentos afines, para prever, diagnosticar, planear, programar, ejecutar y evaluar las funciones esenciales para sustentar la Institución de los servicios de información correspondientes.

Coordinación de incidentes informáticos: Responsable de controlar y solucionar todos los incidentes informáticos que surgen dentro de la Institución.

Departamento: Todas las empresas u organizaciones, están compuestas por áreas o departamentos, los cuales permiten confortar una estructura organizacional basada en centros especializados de actividades y una distribución mejor definida de responsabilidades.

Dirección: Comprende la influencia del administrador en la realización de los planes, obteniendo una respuesta positiva de sus empleados mediante la comunicación, la supervisión y la motivación.

Especialista: Es la persona que se reconoce por conocer y dominar profundamente cierta rama, ciencia u profesión.

Impacto: Es un indicador que nos permite conocer los efectos negativos que ocasiona un incidente en las actividades de la institución. El impacto será mayor en la medida que el incidente afecte negativamente al desempeño de un proceso crítico de la institución, o afecte a un número mayor de usuarios, el impacto de cada incidente esta definido de acuerdo a su escalamiento.

Incidente informáticos: Cualquier evento que ocasione la reducción en el nivel de servicio o la interrupción del servicio informático.

Jefe de sitio: Persona autorizada para tomar decisiones y hacerse responsable de ellas.

Maximizar recursos: Se refiere a maximizar el rendimiento de algo.

Optimizar recursos: Desde un punto de vista informático, la optimización es la búsqueda y el hecho de mejorar el rendimiento de un sistema operativo, programa o dispositivo, a partir de determinados cambios lógicos (software) o físicos (hardware). Mejorar el rendimiento de algo.

Organizar: Es constituir el doble organismo, material y social, de la empresa.

Planeación: Proceso por el cual se obtiene una visión del futuro, en donde es posible determinar y lograr los objetivos**,** mediante la elección de un curso de acción.

Prever: Es escrutar el porvenir y confeccionar el programa de acción.

Prioridad: Es un indicador que permite clasificar los incidentes cuya solución tiene mayor relevancia para la institución.

Usuario: Es la persona que utiliza los servicios informáticos suministrados por La Faculta de Contaduría y Ciencias Administrativas, Alumnos, docente académico, empleados administrativos, público en general.

Seguridad informática: Es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información y sus usuarios.

Solución definitiva en C.I.I.: Es la forma de eliminar de manera permanente la causa raíz de un problema, no siempre existe una solución definitiva. Cuando la solución definitiva es muy costosa o inviable se pude decidir no aplicarla y utilizar soluciones temporales.

Solución temporal en C.I.I.: Es una acción que aminora o elimina el efecto de un incidente, usualmente es la primera solución para restaurar un servicio.

Urgencia: Indicador que permite conocer el tiempo de solución de incidente requerido por el usuario conforma a las necesidades de la institución.

REFERENCIAS BIBLIOGRAFICAS

Titulo: Metodología para una tesis
Autores: Samperi Hdz. Roberto
Editorial: Trillas, 2006

Titulo: Métodos para elaborar una tesis
Autores: Carlos Muñoz Razo
Editorial: Pearson education, 1998

Titulo: Métodos y técnicas de investigación
Autores: Lourdes Munich / Ernesto Ángeles
Editorial: Trillas, 1993

Titulo: Administración de la función informática
Autores: Ricardo Hernández Jiménez
Editorial: Trillas, 2001

Titulo: Planeación y Organización de Empresas
Autores: Guillermo Gómez Ceja
Editorial: McGrawHill, 1994

Titulo: Elementos básicos de la administración.
Autores: R. Ponce
Editorial: Trillas, 1990

Titulo: El proceso administrativo
Autores: Koontz, Harold
Editorial: Mc Graw Hill, 1989

Titulo: Administración de Centros de C.
Autores: Ricardo Hernández Jiménez
Editorial: Trillas, 1997

Titulo: Procedimiento de Administración de Incidentes
Autores: Francisco J. Vega Martínez, Luis R. Juárez Zapatero, Julio Cesar Roldan
Edición N. 2, 2006

Titulo: Fundamentos de seguridad de Redes /Segunda edición
Autor: Eric Maiwald
Editorial: Mc Graw Hill, 2004

Titulo: Redes de computadoras
Autor: Adrew S. Tanenbaum
Editorial: Pearson Prentice may, 2003