41132
22

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

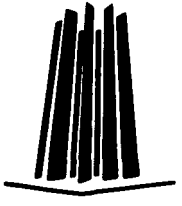
ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN

"SEGURIDAD INFORMATICA EN LOS TALLERES LA PAZ DEL SISTEMA DE TRANSPORTE COLECTIVO METRO"

T E S I S

QUE PARA OBTENER EL TITULO DE:
INGENIERO EN COMPUTACIÓN
P R E S E N T A:

SUSANA FLORES LEAL



ASESOR: ING. GLADIS E. FUENTES CHÁVEZ

MÉXICO, **2003**

1

VERSIDAD NACIONAL
AVFNOMA DE
MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
ARAGÓN
DIRECCIÓN

SUSANA FLORES LEAL
P R E S E N T E.

En contestación a la solicitud de fecha 13 de abril del año en curso, relativa a la autorización que se le debe conceder para que la profesora, Ing. GLADIS EMILIA FUENTES CHÁVEZ pueda dirigirle el trabajo de tesis denominado "SEGURIDAD INFORMÁTICA EN LOS TALLERES LA PAZ DEL SISTEMA DE TRANSPORTE COLECTIVO METRO", con fundamento en el punto 6 y siguientes, del Reglamento para Exámenes Profesionales en esta Escuela, y toda vez que la documentación presentada por usted reúne los requisitos que establece el precitado Reglamento; me permito comunicarle que ha sido aprobada su solicitud.

Aprovecho la ocasión para reiterarle mi distinguida consideración.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
San Juan de Aragón, México, 29 de abril de 2002
LA DIRECTORA

ARQ. LILIA TURCOTTE GONZÁLEZ

ESTUDIOS PROFESIONALES
DIRECCION
ARAGON U N A M

C p Secretaría Académica.
C p Jefatura de la Carrera de Ingeniería en Computación.
C p Asesor de Tesis.

LTG/AJR/lla.

LIC. ALBERTO IBARRA ROSAS
JEFE DE LA UNIDAD ACADEMICA
P r e s e n t e.

Por medio de la presente se hace constar que el alumno **FLORES LEAL SUSANA** con número de cuenta **8817012-5** a concluido satisfactoriamente su trabajo de tesis denominado **"SEGURIDAD INFORMATICA EN LOS TALLERES LA PAZ DEL SISTEMA DE TRANSPORTE COLECTIVO METRO"**.

Se extiende la presente para que el (la) alumno(a) continúe con sus tramites de titulación.

Vo. Bo.

Asesor de tesis
Ing. Gladis Emilia Fuentes Chávez

Jefe de Carrera
M. en C. Jesús Díaz Barriga Arceo

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN

JEFATURA DE CARRERA DE INGENIERÍA EN COMPUTACIÓN

OFICIO:ENAR/JACO/0610/03.

ASUNTO: Asignación de Jurado.

LIC. ALBERTO IBARRA ROSAS
SECRETARIO ACADÉMICO
P r e s e n t e .

Por este conducto me permito presentar a usted el nombre de los profesores que sugiero integren el Sínodo del Examen Profesional del alumno **SUSANA FLORES LEAL**, que presenta el tema de tesis "SEGURIDAD INFORMATICA EN LOS TALLERES LA PAZ DEL SISTEMA DE TRANSPORTE COLECTIVO METRO".

PRESIDENTE:	**MAT. LUIS RAMÍREZ FLORES**
VOCAL:	**ING. SILVIA VEGA MUYTOY**
SECRETARIO:	**ING. GLADIS FUENTES CHAVEZ**
SUPLENTE :	**LIC. MARIA ANGELICA FERIA VICTORIA**
SUPLENTE:	**ING. RODOLFO VAZQUEZ MORALES**

Quiero subrayar que el director de tesis es la **Ing. Gladis Fuentes Chávez**, el cual está incluido con base en lo que reza el reglamento de Exámenes Profesionales de esta Escuela.

Sin otro en particular, me es grato enviarle un cordial saludo.

A T E N T A M E N T E
"POR MI RAZA HABLARÁ EL ESPÍRITU"
San Juan de Aragón, Edo. de México, septiembre 8 del 2003.
EL JEFE DE CARRERA

M. EN C. JESÚS DÍAZ BARRIGA ARCEO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN UNAM

c.c.p. Lic. Ma. Teresa Luna Sánchez.- Jefa del Departamento de Servicios Escolares.
Ing. Gladis Fuentes Chávez. Asesor
Interesado.
JDA*gfc

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
CAMPUS ARAGÓN
JEFATURA DE CARRERA DE INGENIERÍA EN COMPUTACIÓN

Arq. Lilia Turcott González
Directora del Campus Aragón UNAM.
P r e s e n t e .

Por este medio me permito comunicar a usted que revisé la tesis titulada:

SEGURIDAD INFORMATICA EN LOS TALLERES LA PAZ DEL SISTEMA DE TRANSPORTE COLECTIVO METRO

Que presenta el pasante: SUSANA FLORES LEAL

Con número de cuenta: 88817012-5

Para obtener el título de: **INGENIERO EN COMPUTACIÓN.**

Considerando que dicha tesis reúne los requisitos necesarios para ser discutida en el **EXAMEN PROFESIONAL** correspondiente, otorgo mi **VOTO APROBATORIO.**

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"

San Juan de Aragón, Edo., de México, a 5 de Septiembre del 2003

ING. RODOLFO VAZQUEZ MORALES
Revisor de Tesis

M. en C. Jesús Díaz Barriga Arceo
Jefe de Carrera

5

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
CAMPUS ARAGÓN
JEFATURA DE CARRERA DE INGENIERÍA EN COMPUTACIÓN

Arq. Lilia Turcott González
Directora del Campus Aragón UNAM.
P r e s e n t e .

Por este medio me permito comunicar a usted que revisé la tesis titulada:

SEGURIDAD INFORMATICA EN LOS TALLERES LA PAZ DEL SISTEMA DE TRANSPORTE COLECTIVO METRO

Que presenta el pasante: SUSANA FLORES LEAL

Con número de cuenta: 8817012-5

Para obtener el título de: **INGENIERO EN COMPUTACIÓN.**

Considerando que dicha tesis reúne los requisitos necesarios para ser discutida en el **EXAMEN PROFESIONAL** correspondiente, otorgo mi **VOTO APROBATORIO.**

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"

San Juan de Aragón, Edo., de México, a 5 de Septiembre del 2003

MA. ANGELICA FERIA VICTORIA
Revisor de Tesis

M. en C. Jesús Díaz Barriga Arceo
Jefe de Carrera

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
CAMPUS ARAGÓN
JEFATURA DE CARRERA DE INGENIERÍA EN COMPUTACIÓN

Arq. Lilia Turcott González
Directora del Campus Aragón UNAM.
P r e s e n t e .

Por este medio me permito comunicar a usted que revisé la tesis titulada:

SEGURIDAD INFORMATICA EN LOS TALLERES LA PAZ DEL SISTEMA DE TRANSPORTE COLECTIVO METRO

Que presenta el pasante: **SUSANA FLORES LEAL**

Con número de cuenta: **8817012-5**

Para obtener el título de: **INGENIERO EN COMPUTACIÓN.**

Considerando que dicha tesis reúne los requisitos necesarios para ser discutida en el **EXAMEN PROFESIONAL** correspondiente, otorgo mi **VOTO APROBATORIO.**

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"

San Juan de Aragón, Edo., de México, a 5 de Septiembre del 2003

ING. GLADIS E. FUENTES CHAVEZ
Revisor de Tesis

M. en C. Jesús Díaz Barriga Arceo
Jefe de Carrera

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
CAMPUS ARAGÓN
JEFATURA DE CARRERA DE INGENIERÍA EN COMPUTACIÓN

Arq. Lilia Turcott González
Directora del Campus Aragón UNAM.
P r e s e n t e .

Por este medio me permito comunicar a usted que revisé la tesis titulada:

SEGURIDAD INFORMATICA EN LOS TALLERES LA PAZ DEL SISTEMA DE TRANSPORTE COLECTIVO METRO

Que presenta el pasante: **SUSANA FLORES LEAL**

Con número de cuenta: **8817012-5**

Para obtener el título de: **INGENIERO EN COMPUTACIÓN.**

Considerando que dicha tesis reúne los requisitos necesarios para ser discutida en el **EXAMEN PROFESIONAL** correspondiente, otorgo mi **VOTO APROBATORIO.**

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"

San Juan de Aragón, Edo., de México, a 5 de Septiembre de 2003

ING. SILVIA VEGA MUYTOY
Revisor de Tesis

M. en C. Jesús Díaz Barriga Arceo
Jefe de Carrera

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
CAMPUS ARAGÓN
JEFATURA DE CARRERA DE INGENIERÍA EN COMPUTACIÓN

Arq. Lilia Turcott González
Directora del Campus Aragón UNAM.
P r e s e n t e .

Por este medio me permito comunicar a usted que revisé la tesis titulada:

SEGURIDAD INFORMATICA EN LOS TALLERES LA PAZ DEL SISTEMA DE TRANSPORTE COLECTIVO METRO

Que presenta el pasante: SUSANA FLORES LEAL

Con número de cuenta: 8817012-5

Para obtener el título de: **INGENIERO EN COMPUTACIÓN.**

Considerando que dicha tesis reúne los requisitos necesarios para ser discutida en el **EXAMEN PROFESIONAL** correspondiente, otorgo mi **VOTO APROBATORIO.**

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"

San Juan de Aragón, Edo., de México, a 5 de septiembre del 2003

M.A.T. LUIS RAMIREZ FLORES
Revisor de Tesis

M. en C. Jesús Díaz Barriga Arceo
Jefe de Carrera

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN

SECRETARÍA ACADÉMICA

M. en C. JESÚS DÍAZ BARRIGA ARCEO
Jefe de la Carrera de Ingeniería en Computación,
Presente.

En atención a la solicitud de fecha 9 de septiembre del año en curso, por la que se comunica que la alumna SUSANA FLORES LEAL, de la carrera de Ingeniero en Computación, ha concluido su trabajo de investigación intitulado "SEGURIDAD INFORMÁTICA EN LOS TALLERES LA PAZ DEL SISTEMA DE TRANSPORTE COLECTIVO METRO", y como el mismo ha sido revisado y aprobado por usted, se autoriza su impresión; así como la iniciación de los trámites correspondientes para la celebración del Examen Profesional.

Sin otro particular, reitero a usted la seguridad de mi atenta consideración.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
San Juan de Aragón, México, 9 de septiembre del 2003
EL SECRETARIO

Lic. ALBERTO IBARRA ROSAS

C p Asesor de Tesis.
C p Interesado.

AIR/

10

AGRADECIMIENTOS:

A DIOS:

Por haberme brindado la gran oportunidad de existir, de sentirme viva y de estar aquí.

A MIS PADRES: Encarnación y Eustoquia

Por haberme dado la vida, por cuidarme estando enferma, por apoyarme, por tener fé en mí, y sobre todo por alentarme y estar en momentos difíciles en mi caminar por la vida, dándome fuerzas para luchar, por enseñarme que en la vida hay que caminar con coraje, con fuerza y decisión para lograr nuestros más preciados sueños, gracias por darme las bases necesarias y la guía suficiente para tomar mi camino y enfrentarme a la vida, dándome la mejor herencia del mundo.

A MIS HERMANOS: Ricardo, Ebelyn, Alvaro, Sonia, Húmberto, Adriana y Minerva.

Por estar a mi lado en todo este tiempo de esfuerzos, en las buenas y en las malas, en todos aquellos pequeños y grandes instántes de felicidad compartida, por brindarme consejos a tiempo, apoyándome aún sin estar de acuerdo en mis decisiones, pero respetando siempre mi forma de pensar y ser.

CON INMENSO CARIÑO A MIS SOBRINOS (A):

A todos estos pequeños traviesos que con su alegría y optimismo ante la vida, me hacen sentir que todo es posible y que vale la pena vivir, gracias por todo ese que me enseñan a un sin saberlo.

A MIS CUÑADAS (OS):

Por formar parte de mi familia y ser un pilar importante para la unión familiar dentro de este gran núcleo.

A MIS AMIGOS (AS):

A todos ustedes que con palabras de aliento, siempre me apoyaron incondicionalmente y sobre todo tuvieron fé en mí.

A MI HERMOSA HIJA: Gaby

A ti cariño mío, mi más anhelado sueño hecho realidad, por creer en mí, por estar conmigo, por ser mi adorada hija, mi mayor impulso y mi más grande ilusión, a ti chiquita linda por enseñarme a vivir día a día con tu paciencia, cariño, optimismo ante la vida, por comprenderme a tu corta edad pero con un gran madurez que muchas veces me sorprendes con tus comentarios tan acertados desde tu muy particular punto de vista, a ti que siempre me impulsas y me exiges ser cada día mejor. Te dedico este proyecto con todo mi amor.

A RAÚL:

Gracias por apoyarme siempre, por escucharme, alentarme y quererme, por todos esos hermosos recuerdo del pasado en el que me hiciste sentir parte importante y fundamental en tu vida, por compartir parte de tus sueños y tu tiempo a mi lado.

A MIS PROFESORES: A TODOS ELLOS

Por darme las bases necesarias para edificar el inicio del camino y llegar a ser útil y productiva en una sociedad de grandes retos, por mostrarme como abrir las alas y recorrer el mundo.

A MI UNIVERSIDAD:

Por existir y brindarme un espacio en el cual tuve las bases para un buen desarrollo profesional y laboral.

A MI ASESORA: Ing. Gladys E. Fuentes Chávez

Por brindarme parte de su valioso tiempo para lograr desarrollar el presente proyecto y llevarlo a buen fin.

A MI JEFE Y AMIGO: Ing. Gerardo Javier Chacón Cruz

Gracias por creer en mi e impulsarme siempre

Gracias Mil, a todos y cada uno de ustedes que han formado parte fundamental en mi vida.

SEGURIDAD INFORMÁTICA EN LOS TALLERES LA PAZ DEL SISTEMA DE TRANSPORTE COLECTIVO METRO

INDICE

Pág.

Pág.

SEGURIDAD INFORMÁTICA EN LOS TALLERES LA PAZ DEL SISTEMA DE TRANSPORTE COLECTIVO METRO

OBJETIVO GENERAL:

Planear, diseñar, organizar e implementar la Seguridad Informática en la Red de Datos de los programas de mantenimiento y explotación, tanto física como lógica para optimizar los recursos informáticos, a fin de aprovecharlos a su máxima capacidad, mediante el estudio de políticas de control y explotación de los sistemas de información y su correcta y mejor aplicación, beneficiando con ello al Sistema de Transporte Colectivo Metro en sus instalaciones de los Talleres de Mantenimiento "La Paz".

OBJETIVOS ESPECÍFICOS:

- Obtener información mediante un trabajo de campo que consiste en la observación y análisis de actividades y hechos relevantes como son; el uso y explotación del hardware y software, así como del personal usuario.
- Auxiliarse por medio de técnicas y herramientas como son: Muestreos, Entrevistas, Análisis de Inspección, Observación, Documentación y Seguridad de los recursos informáticos.
- Analizar, proponer y diseñar las políticas de trabajo y sus mejores alternativas para el mejor aprovechamiento de los recursos con los que se cuenta.
- Analizar y diseñar una reingeniería de procesos para la disminución de costos operativos de le Red de Datos, aprovechando y optimizando los recursos materiales y humanos disponibles.
- Gestionar ante el responsable de la Unidad Departamental y a su vez con las Autoridades Superiores para lograr, en su medida, un programa de actualización de recursos materiales y la obtención de los recursos financieros para la modernización y adquisición de los equipos informáticos necesarios para dar continuidad al proyecto de Red de datos, evitando con ello el rezago tecnológico y por consiguiente la obsolescencia de los equipos y programas en explotación.

HIPOTESIS

Al lograr la eficiente optimización de los recursos en la administración tendremos con esto reducción en tiempos de espera y agilización del procesamiento de la información para la mejor toma de decisiones.

Al llevar a cabo una buena implementación de Seguridad Informática esta se vera reflejada en el costo-beneficio paulatinamente en los procesos de información.

Con esto se lograra reducir en gran medida los riesgos de seguridad Informática existentes

ANTECEDENTES

Los Talleres la Paz de línea A, del Sistema de Transporte Colectivo – Metro se inauguro el 12 de agosto de 1991, cuenta con una superficie de 18 hectáreas en la cual se encuentra ubicado el Departamento de Servicios Mantenimiento al Material Rodante Férreo, y este a su vez esta compuesto por 6 áreas de mantenimiento y apoyo técnico-administrativo; las cuales son: Coordinación de Mantenimiento Menor, Coordinación de Mantenimiento Electromecánico, Coordinación de Servicios, Ingeniería y Aseguramiento de la calidad al Material Rodante Férreo FM-86, Revisión General y Aseguramiento del Mantenimiento Mayor y el Centro de Información a Talleres.

En un inicio los controles que se llevaban eran en forma documental, empleando máquinas de escribir o controles manuales, pero poco a poco se presentaron nuevas necesidades de control y procesamiento de la información de acuerdo a las actividades generadas, originalmente no existían equipos de cómputo ni un área determinada para el proceso informático, de esta manera se adquirieron equipos informáticos con procesador 386 (en su inicio), e impresoras de matriz de puntos, pero debido al creciente desarrollo se han actualizando los equipos de tal forma que se adquirieron equipos Pentium e impresoras láser, posteriormente se pensó en crear una red informática a fin de poder compartir los recursos tanto de información como de hardware.

Al iniciar con este proyecto informático sólo se contaban con terminales únicas y esto hacia un poco lento el proceso de los trabajos, ya que era todo de forma manual esto es que se tenían que imprimir los reportes, formatos, estadísticas y entregarlos al usuario en información impresa, archivos o bien en diskette, etc. Esto hacia que se incrementaran los costos de operación y se realizaran con lentitud los flujos de la información. Por otra parte se vislumbro la necesidad de realizar un proyecto de RED, con criterios elementales, sistemáticos, ordenados, controlados y críticos, desarrollando un estudio de Seguridad Informática para tener una visión más clara en la cual se comprenderían dos fases, una teórica y otra práctica, haciendo notar que seria un trabajo nuevo en el Departamento de Servicios de Mantenimiento al Material Rodante Férreo, para el área de talleres sobre todo, porque esto sería basado sobre un objeto de estudio, y un análisis de investigación.

La Seguridad en Informática es de suma importancia, ya que la computadora es un instrumento que almacena grandes cantidades de información, además de manejar información confidencial para algunos usuarios, o áreas, y esta es susceptible de ser usada o divulgada a personas que hagan mal uso de ella, además de que es la administración y protección de recursos con los que cuentan los Talleres La Paz del Sistema de Transporte Colectivo –Metro-, por lo cual es importante proteger el patrimonio informático entendiéndose por este; instalaciones, equipos, e información almacenada en los equipos de cómputo.

En el presente trabajo se analiza la estructura, esquemas y forma de trabajo actual; en la cual se pretende, al finalizar, implantar una forma y metodología que beneficie a los Talleres La Paz, logrando con ello la optimización de todos los recursos con los que cuenta actualmente, para esto iniciaremos con pruebas de campo que nos ayuden a delimitar los puntos clave y ver en que aspectos hay debilidades, y poderlas convertir en oportunidades, para esto alternaremos con los mismos usuarios, para percibir más de cerca la problemática, además de analizar la información (documentación) que existe en el control de documentos, hardware y software, no obstante, como de momento es poco el control que se tiene en las diversas áreas, nos apoyaremos en la tecnología informática para contar, con una mejor distribución de datos y agilizar los procesos, ya que en la actualidad estos se llevan acabo en forma manual, haciendo lento el avance de controles y que algunas personas abarquen más funciones de las que les corresponden y por la misma situación, descuidando otras actividades que podrían beneficiar y quizá hasta reducir actividades pero que debido a las cargas de trabajo no se han analizado correctamente, pero se pretende mediante el presente documento, proponer soluciones concretas, algunas posiblemente serán a corto, mediano o largo plazo.

JUSTIFICACIÓN

Debido a la creciente necesidad de todas, y cada una de las empresas, para llevar un mejor control y seguridad de los medios informáticos, es necesario aplicar los últimos avances tecnológicos para obtener grandes beneficios por medio de la Seguridad Informática.

La informática esta orientada a facilitar el trabajo y aprovechar los recursos con los que se cuenta, además de que la realización del presente proyecto va ayudar a brindar soluciones para la consecución de los objetivos de los talleres la Paz, la informática en conjunto con el estudio de la Seguridad Informática dan soporte para una mejor toma de decisiones que aunado a los conocimientos adquiridos durante la carrera nos brinda grandes beneficios con los cuales se alcanzarán; mayor agilización y control de la información y los recursos, logrando con esto promover la eficiencia del personal usuario mediante medidas de seguridad que ayudaran a tener un mejor control con la información y los equipos.

Algunas de las actividades a contemplar de la Seguridad Informática serán:

La seguridad física de las instalaciones y equipos en las cuales se contemplaran posibles inundaciones, incendios, explosiones, corte de líneas o de suministros, equipos mal instalados.

Se vigilará que el desarrollo de aplicaciones sea en un entorno seguro y que además se implementen controles de seguridad de protección.

Así mismo esta contemplada la seguridad lógica para que el usuario indicado tenga acceso únicamente a los recursos que tenga autorizado y realizar sólo las funciones permitidas, como podrán ser lectura, modificación, ejecución, borrado, copias, etc.

El entorno de producción, como tal explotación más técnica de sistemas, y con especial énfasis en el cumplimiento de contratos en lo que se refiere a protecciones, a terceros cuando se trata de entidad que presta servicios, como el que se recibe de otros.

Protección de datos, en cuanto a los datos en general según la clasificación que exista, la designación de propietarios y los riesgos a que estén sometidos.

En comunicaciones y redes se revisará y modificará en caso de ser necesario la topología, tipo de comunicaciones, protecciones ante posibles virus.

Continuidad de operaciones, dígase seguimiento inicio y fin de las mismas.

Se desarrollará la metodología de investigación de campo por medio de encuestas, entrevistas, visitas con los usuarios formales e informales, análisis de fallas y solución a las mismas.

Esta inquietud de desarrollar y analizar la seguridad informática en los talleres la Paz del STC-Metro surgió a partir de observar que se han estado presentando diversas fallas sistemáticas en lo que concierne a la red informática como lo es pérdida de información, saturación de espacio en disco por falta de mantenimiento en los equipos, carencia de conocimientos del personal usuario, contaminación de virus, uso inadecuado de la información debido a la ausencia de controles de acceso de seguridad, alteración de configuración por desconocimiento, mal uso del equipo informático, carencias de actualizaciones tanto en hardware como en software, duplicidad de funciones en algunos casos, lentitud en los procesos, entre otros.

Los beneficios que se lograran serán resolver poco a poco todos y cada uno de las fallas presentadas, es decir, las debilidades convertirlas en oportunidades de desarrollo y funcionalidad.

Ésta se trata de una red de área local (Lan) y es muy usual en oficinas o en un solo edificio, en la cual todos los recursos se encuentran a cargo del mismo servidor, con una topología de tipo estrella que es la estructura en que están interconectadas las estaciones de trabajo en la red.

La topología de tipo estrella se basa en unir todas las estaciones en un solo punto (máquina central) la principal ventaja que ofrece esta topología es que disminuye considerablemente el tráfico de información en la red, la cual utiliza un sistema operativo de Windows NT capaz de correr varias aplicaciones de Windows escrito completamente en código de 32 bits.

Actualmente las computadoras conectadas pueden compartir los recursos de todas las demás estaciones de trabajo, sin importar en donde se encuentren dentro de la red. También es posible imprimir en una impresora conectada a otra computadora o modificar un archivo ubicado en el disco duro de otro equipo informático (por medio de compartición de archivos y recursos).

También se esta utilizando una estructura determinada Arquitectura Cliente/Servidor, el cual significa a grandes rasgos, que algunas computadoras de la red actuaran como servidores de algún recurso (archivos, impresión, base de datos etc.) por ser utilizados por otras computadoras que se denominan cliente.

Este modelo de operación disminuye el tráfico en red facilitando la coordinación de esfuerzos independientes y centralizar operaciones críticas. De esta forma se hace imperativa la necesidad del poder que ejercen los equipos de cómputo. La importancia de este proceso es que la información sea utilizada sólo por la gente precisa y en el lugar adecuado para ello haciendo uso de las capacidades del personal usuario, conocimiento y perfil de puesto que desempeña.

INTRODUCCIÓN

El presente trabajo proporciona el análisis y diseño del sistema para el control de la información, en los Talleres La Paz del Sistema de Transporte Colectivo Metro, en el cual se realizará un análisis de la forma de trabajo en cuanto a seguridad informática en la red interna específicamente de las instalaciones en el área de Talleres la Paz, el cual actualmente cuenta con aproximadamente 15 equipos de cómputo distribuidos en las áreas de los Talleres, los cuales interactúan por medio de una red LAN y un servidor de red con Sistema Operativo Windows N.T Versión 4.0, y de la cual se puede decir que la topología Física es lineal, utilizando concentradores de comunicación, asimismo, la topología lógica de la red es de tipo estrella, debido a su flexibilidad de manejo y posibilidad de crecimiento.

Se hará una descripción de cada etapa, explicando en cada una de ellas la Seguridad Informática en los Talleres La Paz, así como sus principales características, alcances, objetivos, requerimientos, usuarios, organigramas de organización y de personal, de equipos informáticos, y la propuesta de implantación de un sistema, El cual se ha dividido en **5 capítulos** que serán desarrollados de la siguiente manera:

En el Primer Capítulo, Iniciaremos con los antecedentes informáticos históricos de los Talleres la Paz, la distribución de los equipos informáticos, así como un diagnóstico general de la RED informática interna de los talleres La Paz, con la finalidad de tener un panorama general de la situación actual, y ver los cambios conforme se va avanzando en el proyecto.

El Segundo Capítulo, abarca la planeación referente a la forma de trabajo que emplearemos para desarrollar este proyecto, que será por medio de una matriz de riesgos y un plan detallado de seguridad informática, para definir responsabilidades, tiempos y características, componentes, ventajas, y desventajas, así como los beneficios al concluir el proyecto.

El **Tercer Capítulo**, es la implementación y la metodología de acuerdo al usuario, analizando de cerca las actividades que realiza y las funciones que desarrolla además de un plan de trabajo previamente elaborado.

El **Cuarto Capítulo**, denominado desarrollo e implementación, se mencionarán las áreas seleccionadas de trabajo; también se realizará un informe de Seguridad en informática, así como la asignación de responsabilidades y tiempos para cada acción, recomendaciones, acciones determinadas y compromisos, basados en un plan de trabajo, y como complemento, la aprobación final. Ya que una vez detectadas las necesidades y problemáticas actuales, se contemplarán las soluciones, eligiendo aquellas que se adapten de mejor manera a las necesidades de los usuarios y de los cuales será de gran importancia darle el seguimiento adecuado para su buen desarrollo.

El **Quinto Capítulo**, es la documentación, en la cual se encuentra el proceso de desarrollo del proyecto seguridad Informática en los talleres la paz del Sistema de Transporte Colectivo Metro, así como un documento de aprobación formal, con las firmas por parte de los usuarios u autoridades, y compromisos que serán el respaldo y apoyo al proyecto de parte de la alta dirección, para que este tenga un buen seguimiento y resultados planeados, la aplicación de la solución final, ya que con ella se verificara que se ejecuten periódicamente los procedimientos aprobados y documentados para la obtención de resultados.

Finalmente; mencionaremos las conclusiones a las que se llegó con la elaboración de este proyecto para la realización de la presente tesis.

CAPÍTULO I

ANALISIS PRELIMINAR

CAPÍTULO I ANÁLISIS PRELIMINAR

En la presente Tesis surgió la inquietud de buscar un mejor nivel de seguridad informática en los Talleres la Paz del Sistema de Transporte Colectivo (ubicándonos únicamente en la red informática interna de los talleres la paz) en la cual me he encontrado colaborando como parte activa en este organismo, además de ser egresada de la Carrera de Ingeniería en Computación. Mi inquietud me lleva a analizar y plantear una solución idónea para los diversos problemas que han ido surgiendo durante mi estancia, los cuales se encuentran detallados más adelante con la metodología FODA (Fortalezas, Amenazas, Debilidades y Oportunidades), la cual considere la mejor alternativa para obtener datos relevantes que me permitieran tener un panorama más amplio y de esta manera estar en posibilidad de brindar soluciones a corto plazo.

Hablando de la Red Interna de los talleres la paz, se puede decir que es la que se encarga de realizar las diversas programaciones de mantenimiento de trabajo en los trenes durante todo el año, además de la realización de metas anuales, programas operativos, presupuestos, limpiezas, Revisión Mayor y Menor, Mantenimientos electromecánicos a fin de tener en óptimas condiciones los vehículos auxiliares entre otros, programas de mantenimientos semanales, descargas de trabajos, control de reportes cíclicos, sistemáticos, kilometraje, avance de actividades etc. Por lo tanto se puede decir que es la parte medular en la que se concentra toda la información de requerimientos y necesidades del parque vehicular (trenes) generada. En el Departamento de Servicios de Mantenimiento al Material Rodante Férreo para así reportar a instancias superiores del organismo.

Por todo ello podemos decir que es de suma importancia lograr un buen control de seguridad que coadyuve al resguardo y protección de la información que en ella se genera además del grado de confidencialidad con el se debe tratar, ya que las actividades y los procesos de trabajo se incrementan día a día y el manejo de la información en la red interna se vuelve cada vez mayor.

Esta red interna en los talleres la paz se ha ido adecuando poco a poco de acuerdo a las necesidades de información generadas y con los recursos de hardware y software que se han adquirido a través del tiempo. Cabe mencionar que anteriormente la Gerencia adquirió un software de mantenimiento denominado Max&Maint con el cual se pretendía agilizar los procesos de trabajo pero que debido a la falta de recursos humanos, materiales y de capacitación además del continuo incremento de actividades se ha dejado a un lado y es por ello que es necesario cubrir la parte de la seguridad a los recursos que actualmente se encuentran en explotación, protegiendo los intereses de la empresa, así como de información para que este se encuentre disponible en el momento que se requiera sin mayores contratiempos además de ser precisa, veridica y oportuna.

Es importante aclarar que si se logra contar con el apoyo de los usuarios en general avanzaremos adecuadamente logrando la seguridad en un mediano plazo reduciendo significativamente los puntos de riesgo.

Para ello se considera importante analizar todos los puntos clave, como es la detección de riesgos y que se analizara con el formato FODA, el cual se utilizará como herramienta de trabajo; asimismo un análisis de riesgos y áreas de oportunidad detallándola con una matriz de riesgos, de igual manera las políticas actuales de la empresa y las áreas de oportunidad presentes que se derivan de la función informática.

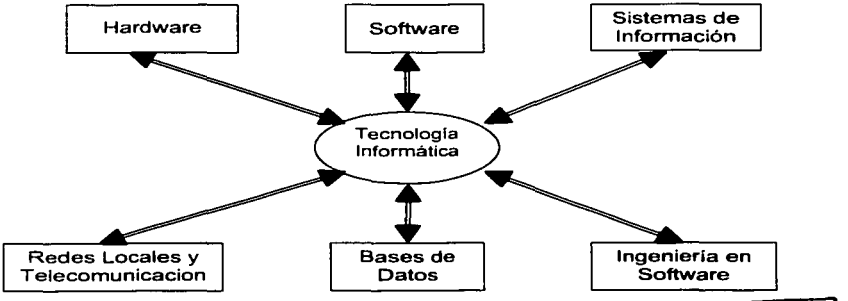
La función de la seguridad informática es entender los puntos débiles y fuertes de la función informática desde el punto de vista de usuarios comunes y los directivos. El cual comprende los siguientes puntos:

- **Diagnóstico del sistema informativo:**
  Comprende la misión de la empresa, actividad, áreas de proceso, organigramas de organización, relación entre las áreas internas y además la importancia que se le da a la Seguridad informática dentro de la empresa.

- **Diagnóstico de Informática:**
  Se dará a conocer la misión, meta, objetivos, estructura e importancia de la informática, los tipos de servicios que brindan (evaluación, adquisición, instalación y reemplazo de equipo de cómputo, capacitación a personal usuario, adquisición de software etc.) así como el planteamiento de aspectos de control (políticas y procedimientos con respecto a informática, descripción de puestos y funciones, evaluación de desempeño, políticas y procedimientos para el desarrollo de aplicaciones, seguridad, planes de contingencia, hardware software, redes entre otros.

IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA EN LOS TALLERES LA PAZ DEL SISTEMA DE TRANSPORTE COLECTIVO -METRO-

La información constituye uno de los activos más importantes en toda empresa, independientemente de su actividad económica, política o social, por lo tanto la seguridad en Informática es una herramienta estratégica que brinda rentabilidad y ventajas competitivas a la empresa cuando son enfocadas debidamente, tomando en cuenta los recursos que se tienen dentro de la misma y estableciendo los mejores sistemas de información y su eficiente explotación, para ello a continuación se muestra un esquema de la forma en que interactúan la Tecnología Informática con el apoyo de otros recursos.



ESTRATEGIAS Y PÓLITICAS DE ACCIÓN PARA LA IMPLANTACIÓN DE SEGURIDAD INFORMÁTICA

- Formalizar la Seguridad en Informática a través de :
  - Justificación de la función informática.
  - Presentación del plan de seguridad.
  - Aprobación del proceso y del plan.
  - Difusión de la seguridad.
- Proporcionar a la empresa un proceso de seguridad en Informática permanente con el objeto de garantizar el buen funcionamiento que se lleva a cabo en cada etapa, con resultados comprobables:
  - Que la seguridad, políticas y procedimientos se orienten hacia los recursos de la informática y hacia la información que se maneja, haciéndolo de manera confiable y eficiente.
  - Apoyo a los objetivos de la empresa (talleres La Paz) previamente analizados.
  - Verificación física del uso y tecnologías que se requieren y justifica cada área de los Talleres La Paz.
  - Existencia de un proceso de evaluación y justificación de cada proyecto de investigación con respecto a la función informática.

POLÍTICAS DE ACCIÓN:

- Crear conciencia en el personal de la importancia de la informática.
- Informar del proyecto, objetivos, beneficios y áreas que contempla la Seguridad en informática, para su aprobación a la Jefatura del Departamento responsable de las instalaciones de los Talleres "La Paz".
- Dar conocimiento a usuarios y personal del grado de compromiso y participación que se requiere para que el proyecto se concluya exitosamente
- Coordinar formalmente visitas y reuniones de trabajo necesarias con el personal usuario y de informática, involucrado en cada proyecto.
- Entregar a las estructuras de mandos superiores de manera general y oportuna, informes detallados de cada etapa del proyecto, aprobados por el comité de trabajo.

PLANEACIÓN DE SEGURIDAD EN INFORMÁTICA Y METODOLOGÍA PARA SU DESARROLLO E IMPLANTACIÓN

Planeacion de la Seguridad en Informática: Se define como un proceso que elabora y formaliza una serie de proyectos a corto, mediano y largo plazo orientados a la evaluación y revisión oportuna de todos los componentes inherentes a informática.

La planeación de este proyecto cuenta con los siguientes elementos:

- Etapa de análisis y planeación.
- Formalización de las actividades.
- Análisis de costo/beneficio.
- Resultados esperados por cada actividad y etapas.
- Responsables de cada actividad o etapa.
- Involucrados o participantes.
- Revisiones formales, informales y documentales.

- Técnicas para ejecutar actividades.
- Herramientas para realizar cada una de las actividades del proyecto.
- Necesidades generadas en cada área.

PUNTOS PARA LA ELABORACIÓN DE UN PLAN MODELO DE SEGURIDAD EN INFORMÁTICA

Crear o formalizar un comité de control y seguimiento integrado por la alta dirección y los representantes directos de la Seguridad informática.

Analizar las necesidades de la empresa (talleres La Paz), de informática y de Seguridad en informática de manera conjunta con objeto de ver la relación o impacto que tienen entre sí.

Establecer fechas de reuniones formales e informales para dar seguimiento a los planes de compromiso conjunto.

ASPECTOS GENERALES DEL DIAGNÓSTICO DEL ÁREA A AUDITAR

- Obtener una lista de los principales sistemas de información utilizados por los usuarios y su objetivo.
- Tomar como base las experiencias, comentarios y sugerencias de los usuarios de cada sistema.
- Registrar las fallas o eventos más comunes de cada sistema.
- Recabar informes de desempeño hechos con anterioridad a usuarios, analistas u otro personal.
- Anotación de fechas de instalación de sistemas y fechas de actualización (bitácora de trabajo)
- Revisar la configuración del equipo (hardware y software).

OBJETIVOS DEL USO DE UNA METODOLOGÍA DE SEGURIDAD EN INFORMÁTICA

- Definir clara y detalladamente los requerimientos y condiciones que justifiquen cada proyecto.
- Las limitaciones y/o carencias de políticas y procedimientos existentes en las áreas relacionadas con la informática, que generen necesidades para determinar la seguridad existente.
- Definir etapas o secuencias del proyecto.
- Especificar funciones y responsabilidades del personal que participaran en los proyectos de seguridad en informática (líder del proyecto, usuarios y personal de las áreas de apoyo al proyecto).
- Definir técnicas y herramientas mínimas para cada etapa del proyecto de seguridad en informática (muestreos, entrevistas, cuestionarios, inspecciones/observaciones documentación, software de seguridad, análisis de sistemas, lenguajes de programación aplicados, software de administración, equipo de cómputo disponible).

FORMALIZACIÓN DE UN COMITÉ DE CONTROL DE SEGURIDAD DE SEGUIMIENTO INTEGRADO POR:

RESPONSABLES DEL PROYECTO DE SEGURIDAD EN INFORMÁTICA

A continuación se enlista los cargos del personal encargado de cada una de las Coordinaciones que conforman el Departamento de Servicios de Mantenimiento al Material Rodante Férreo y que a su vez cuentan con equipos de cómputo para la realización de actividades, además de compartir recursos y hacen uso de la red informática.

CARGO	ÁREA
Jefe del Departamento	Departamento de Servicios de Mantenimiento al Material Rodante Férreo
Coordinador de Proyectos B N-13	Mantenimiento Menor
Coordinador de Proyectos B N-13	Mantenimiento Electromecánico
Supervisor de Mantto. A N-10	Coordinación de Servicios al Material Rodante
Jefe de Proyectos A N-12	Centro de Información a Talleres (C.I.TA)
Coordinador de Proyectos B N-13	Aseguramiento de la Calidad al Mantenimiento Mayor FM-86
Coordinador de Proyectos B N-13	Ingeniería del Material Rodante

La única forma de asegurar un compromiso es por medio de la participación de todos los afectados por las medidas de seguridad en su diseño y aplicación.

Con este comité se pretende formar un equipo de trabajo que coordine y auxilie en el apoyo informático de los talleres mediante reporte de anomalías y fallas que encuentren en sus equipos de cómputo. Esto es con el fin de reunir esta información y enfocarla a un solo punto y poder darle pronta solución a los problemas que surjan.

Es importante hacer conciencia hacia el personal para lograr la asignación dedicada de una persona que se encargue directamente de las labores propias de la informática, así como de un administrador de red a fin de poder brindar un mejor seguimiento en cada una de las situaciones que se presenten.

(Ver anexo No. 4)

Visto Bueno

Ing. Gerardo J. Chacón Cruz
Jefe del Departamento de Servicios de Mantenimiento
Al Material Rodante Férreo

ANALIZAR DE MANERA CONJUNTA CON EL PERSONAL INVOLUCRADO Y RESPONSABLES DE ÁREA (Formato FODA)

Objetivo: Identificar al personal clave que desarrolla actividades dentro del ámbito informático para tener un panorama más amplio del estado actual de los equipos, programas y recursos en explotación, para ello es necesario conocer las tendencias que tarde o temprano puedan influir o determinar acciones en forma directa.

Para esto se diseño un formato en el cual de manera clara y concisa nos mostraran las principales fallas que presenten los equipos informáticos en los Talleres la Paz.

DISEÑO DE FORMATO DEL CUESTIONARIO A SER APLICADO A LOS USUARIOS

ANÁLISIS DE FUERZAS, OPORTUNIDADES, DEBILIDADES Y AMENAZAS (FODA) EN LAS ÁREAS DE LOS TALLERES LA PAZ

NOMBRE DEL USUARIO: (Persona que hace uso del equipo) **FECHA:** (fecha de elaboración)

ÁREA DE TRABAJO: (nombre del área en la que se encuentra el equipo) **NOMBRE DEL NODO:** (nombre asignado al equipo)

Este análisis tiene la finalidad de identificar las circunstancias internas que influyen en el área de informática representadas por:

FUERZAS: Se le denomina a todas aquellas características con las que favorecen el área informática.

DEBILIDADES: Es todo aquello que se observe como carencias y deficiencias que entorpecen la labor informática.

Así mismo se identificarán aquellas causas externas que afectan a la unidad informática constituidas por:

AMENAZAS: Como lo son el mal uso de la información, mal manejo de equipo etc.

OPORTUNIDADES: Son aquellas que benefician para un mejor aprovechamiento de los recursos informáticos.

Al final lo que se busca es convertir estas debilidades en oportunidades y las amenazas en fuerzas.

INSTRUCCIONES: Llene cada uno de los recuadros según su opinión y experiencia con los equipos de cómputo.

FORTALEZAS	**AMENAZAS**
ACTIVIDADES EFICACES; PARA PRODUCIR UN EFECTO DESEADO, ADEMAS DE QUE EL RESULTADO QUE BRINDE SEA EL OPTIMO	EXTERNAS Y/O INTERNAS
DEBILIDADES	**OPORTUNIDADES**
NO ES NI EFICAZ, NI EFICIENTE O BIEN RECURSOS QUE NECESITA PERO QUE NO POSEE	RECURSOS RENTABLES

Una vez aplicado el formato anterior (FODA) con las áreas usuarias, sirvió para determinar las causas principales fallas que están presentes en la Red Informática para las cuales se aplicarán las medidas de seguridad necesarias a fin de poder tener un mejor control y conocimiento de fallas.

El realizar este análisis, sirvió para evaluar una posibilidad real de lo que efectivamente se puede hacer, el cual constituye un instrumento fundamental para analizar y revalorar los objetivos del entorno informático y así poder determinar de forma precisa, las estrategias a seguir, lo que verdaderamente importa es poder apoyar las Fortalezas y Oportunidades y de esta manera disminuir las Amenazas y Debilidades.

DESGLOSE DE RESULTADO DE ENCUESTAS (ver los cuestionarios aplicados en el Anexo 1)

- **FORTALEZAS**
  - La manera en que se comparte la información hace que se agilicen los resultados logrando con ello un mejor control y mayor eficiencia.
  - Información actualizada
  - Se cuenta con una impresora láser jet 1200 series y una hewlett packard 5mp en red, en algunos otros equipos se cuenta con impresora de matriz de puntos compartida,, además de contar también con otros recursos compartidos como la unidad de CD Rom, dándonos ventajas considerables para realizar algunas actividades en equipos con los que no se cuenta con este dispositivo.

- **AMENAZAS**
  - Falta de un control de accesos a la red eficiente.
  - Falta de archivo de claves en común acuerdo con el área usuaria.
  - Inexistencia de una herramienta de mantenimiento para el servidor.
  - Asignación de espacios en servidor con un alto control y seguridad para los usuarios.
  - Respaldos actualizados y programados a fin de mantener la integridad de los mismos.
  - Fácil ataque con virus o hackers.
  - Introducción de un posible virus por falta de actualización del software antivirus.
  - Que los equipos se encuentren en zonas de polvo y que esto a la larga puede dañarlos.
  - Falta de claves para acceso a red y hacer mal uso de la información
  - Que personas con desconocimiento de los equipos alteren la información.
  - Introducción de diskette que no pertenecen al área y pudieran tener virus.
  - Instalación de juegos que podrían contener virus o modificar la configuración del equipo.

- **DEBILIDADES**
  - Acceso muy fácil de los nodos a toda la información de la red.
  - Falta de jerarquía en los accesos de red
  - Inexistencia de catalogo de jerarquías.
  - Falta de depuración de archivos temporales en los equipos.
  - Mala configuración de los equipos por desconocimiento
  - Alteración de la información por falta de contraseñas de acceso hacia la red.
  - Equipos informáticos sin tecnología de vanguardia
  - Falta de actualización de Software.
  - Falta de hardware y software original y actualizado necesario para un área informática

- **OPORTUNIDADES**
  - Capacitar a los usuarios conforme sea necesario para el uso de la red.
  - Verificación periódica de todos los nodos y sistemas implantados, conforme al programa de trabajo que se establezca.
  - Mayor control de acceso para un mejor uso de la información.
  - Verificación del uso de software acorde a las necesidades de cada área en especifico
  - Listado de uso de cada uno de los equipos informáticos y responsables
  - Tener acceso a la información actualizada con las demás áreas de trabajo.
  - Disponibilidad de archivos generados por otros usuarios para agilizar el movimiento de la información.
  - Guardar archivos de importancia y de interés común para otras áreas en el servidor.
  - Tener respaldos en el servidor sirve como protección contra algún posible daño que pudiera sufrir alguno de los equipos
  - Tener una impresora de red y que sirva para todos los equipos que no tiene en que realizar sus impresiones.
  - Acceso a la información las 24 hrs. del día, los 365 días del año en algunos equipos con información vital e importante.

ANALIZAR LOS PROCESOS DE TRABAJO DE LOS TALLERES Y SUS ÁREAS RESPECTIVAS (ORGANIZACIÓN Y ACTIVIDADES ACTUALES)

A continuación se muestran las actividades llevadas a cabo por cada área, para ver su distribución y organización de la información misma que es aplicada en cada uno de los equipos de la red para tener un panorama más amplio de las funciones informáticas realizadas por el departamento.

- ***COORDINACIÓN DE MANTENIMIENTO MENOR***

  - Aplicación del software para el control de averías de los trenes de Línea "A"
  - Control, seguimientos, estadísticas y expedientes de averías.
  - Seguimiento de la disponibilidad de trenes.
  - Estudio y análisis de vida útil de los equipos del material rodante férreo.
  - Retroalimentación de funcionamiento de equipos (Análisis de equipos con mayor índice de fallas).
  - Estadísticas de la afectación del servicio y fiabilidad.
  - Frecuencia de fallas de los trenes de Línea "A".
  - Análiisis para el desarrollo del software para el mantenimiento preventivo a boguies y cajas.
  - Desarrollo del catálogo de partes de los equipos del Material Rodante Férreo
  - Control de órganos.
  - Control y estadísticas del mantenimiento sistemático boguie y cajas modelo FM-86 y FM-95A.
  - Control de kilometraje por tren para la programación de mantenimientos. Preventivo y correctivo del mismo y mantenimiento mayor.
  - Programación y control del mantenimiento preventivo sistemático a boguies y cajas modelo FM-86 y FM-95A.

- ***MANTENIMIENTO ELECTROMECÁNICO (MECÁNICO, MECÁNICA Y MAQUINADO)***

  - Aplicación del software para el control de los equipos.
  - Programación de mantenimiento preventivo
  - Control y seguimiento del mantenimiento preventivo.
  - Controles de refacciones y partes.
  - Seguimiento de la operación de los equipos.
  - Desarrollo del catálogo de partes.
  - Control y seguimiento del mantenimiento correctivo.
  - Requerimientos de herramientas para el mantenimiento.
  - Requerimiento de recursos materiales para las actividades de mantenimiento.
  - Estudio y análisis de vida útil de los equipos.
  - Control de los trabajos en garantía.
  - Reporte de actividades mensuales.

- ***MANTENIMIENTO MAYOR***

  - Análisis de las actividades prioritarias del Material Rodante modelo FM-86 y FM-95A.
  - Estudio de los recursos materiales y refacciones.
  - Estudio de las herramientas de trabajo necesarios para el Mantenimiento.
  - Estudio de los equipos requeridos.
  - Análisis de las cargas de trabajo.
  - Análisis y programación de los carros de trenes.
  - Levantamiento e inventario de los órganos en rotación de carros modelo FM-86 y FM-95A.
  - Control de los trabajos en garantía de los equipos del material rodante férreo por servicio externo de los modelos FM-86 y FM-95A.
  - Procedimiento para el control de órganos en rotación.
  - Generación de actividades realizadas mensualmente

- ***COORDINACIÓN DE SERVICIOS AL MATERIAL RODANTE***

  - Procedimiento para el control de limpieza de trenes. (menor, exterior, profundo, toldo, pulido y encerado, con máquina lavadora, instalaciones, talleres y fosa de visita Pantitlán).
  - Control de actividades de limpieza de instalaciones y su eficiencia.
  - Control de personal asignado a la limpieza de las instalaciones mediante reportes de los supervisores.
  - Control de actividades de limpieza menor, profunda, exterior con la máquina lavadora de trenes.
  - Control de las actividades de limpieza
  - Mantenimiento de toldos de trenes.
  - Mantenimiento, pulido y encerado de carrocerías y cristales de trenes.
  - Procedimientos de trabajo de asistencia del personal, vacaciones, tiempo extra.
  - Elaboración de requisiciones.
  - Control de pruebas de laboratorio
  - Seguimiento de capacitación.
  - Control de asistencia.
  - Desarrollo y aplicación de software de control de vacaciones del personal.
  - Seguimiento y control de tiempo extra.
  - Actualización de plantilla del personal sindicalizado y de confianza
  - Actualización del organigrama del departamento.
  - Elaboración de metas mensuales del departamento.
  - Informes diarios, semanal, quincenal y mensual.
  - Elaboración y seguimiento de metas programadas anualmente para el departamento.

- ***CENTRO DE INFORMACIÓN A TALLERES***

  - Apoyo a todas las áreas de trabajo las 24 hrs. del día, los 365 días del año.
  - Atención de averías y canalización de las mismas
  - Control de asistencia del personal de limpieza
  - Control y atención de reportes de trabajo y/o canalización a las áreas correspondientes.

- ***INGENIERÍA AL MATERIAL RODANTE FERREO***

  - Capacitación de trenes modelo FM-95A.
  - Documentación técnica de trenes modelo FM-95A.
  - Catálogo de trenes modelo FM-95A.
  - Relación de pendientes de equipos de la empresa ALSTOM
  - Liberación del lote de refacciones contractuales
  - Variaciones en alimentación de alta tensión. Consumo de energía trenes FM-86 y FM-95A
  - Previa a reunión de representantes técnicos
  - Análisis de innovación tecnológica "ruedas resilentes" montadas en trenes
  - Documentación técnica FM-95A
  - Motores de tracción trenes FM-95A
  - Protocolos para la realización de pruebas de entrada de trenes FM-86 y FM-95A.
  - Reporte sobre anomalías en engrasado de motores de tracción, trenes FM-95A
  - Seguimiento de carbones "EISA" en motores de tracción FM-86.
  - Seguimiento de prueba de innovación tecnológica "ECONOV" en mcp, trenes FM-86.
  - Participación en reuniones para realizar el análisis general de la innovación tecnológica "ruedas resilentes"
  - Verificación y análisis estadístico de las cotas relacionadas con las ruedas resilentes a prueba
  - Modificaciones en block "pm"
  - Modificaciones en manipuladores de cabina trenes FM-95A.
  - Reemplazo de flechas de disyuntores
  - Actualización de documentos técnicos FM-95A por modificaciones.
  - Refacciones FM-95A no contractuales.
  - Problemática de rodamientos dañados en ventiladores onix.
  - Averías en trenes FM-95A
  - Fallas sistemáticas
  - Medición del consumo de energía en trenes FM-86 y FM-95A
  - Variaciones en la alimentación de alta tensión en línea
  - Cerraduras electromagnéticas de puertas cabina-salón pasajeros
  - Seguimiento de Innovaciones tecnológicas de las ruedas resilentes"
  - Manuales de mantenimiento trenes FM-95A
  - Sistema de comunicación remota (SICOR)
  - Motores de tracción
  - Sobre consumo de balatas

ANTECEDENTES INFORMÁTICOS

INTRODUCCIÓN

El presente capítulo tiene por objeto mencionar la plataforma e infraestructura que se ha utilizado para formar la Red Informática en los Talleres la Paz del STC-Metro, es decir, analizar y describir las herramientas de software y hardware, así como la arquitectura que se utiliza y una breve reseña informática.

¿QUÉ ES UNA RED?

Una red empieza desde la conexión de dos o más computadoras conectadas entre sí por medio de un cable, de tal manera que estas puedan intercambiar información, compartir componentes y recursos. Las redes son llamadas con frecuencia LAN es un acrónimo de Local Área Network o red de área local. Cualquier computadora que este conectado en una red local se denomina LAN.

¿PARA QUE SE NECESITA UNA RED?

Principalmente es para compartir información, también para tener acceso a la misma desde cualquier estación de trabajo que se encuentre conectada a la red, ya que esto facilitara el procedimiento de la información deseada y en el lugar en el que se requiera. Específicamente las redes son para compartir tres cosas: archivos, recursos y programas.

Archivos: las redes permiten compartir información con otras estaciones de trabajo de red. Dependiendo de cómo este montada la red, se pueden compartir archivos de tres maneras.

El modo más directo es enviar un archivo desde una estación de trabajo hasta la estación de trabajo a otra. Otra sería almacenar el archivo en un lugar intermedio para que después tener acceso a el en otro equipo. Y por último sería almacenar permanentemente el archivo en ese lugar intermedio diferentes usuarios puedan obtener y modificar el archivo cada vez que lo quieran.

Recursos: se pueden compartir algunos recursos computacionales como disco duro o impresora de tal manera que todas las estaciones de trabajo dentro de la red puedan acceder o emplear alguno de ellos.

Las unidades de disco también pueden ser recursos compartidos, una unidad debe definirse como recurso compartido para poder compartir archivos con otros usuarios.

También es posible compartir otros recursos como unidades de CD ROM (son dispositivos que almacenan gran cantidad de datos y son útiles principalmente para guardar bibliotecas de imágenes o enciclopedias) MODEMS (permiten acceder a otros computadoras que están fuera de la red mediante la red telefónica), CARTUCHOS (cinta magnética,) los cuales pueden utilizarse como un medio de respaldo para la información.

Programas y aplicaciones: consiste en poner las aplicaciones o programas en un disco compartido, es mejor que tener copias de programas en cada una de las estaciones de trabajo ya que es más fácil, tener una copia de cualquier programa que muchas. (Otra ventaja es lo limitativo de la cantidad de licencias por software, debido al costo que ello genera).

BENEFICIOS DE LA RED

Muchas organizaciones tienen una cantidad muy importante de computadoras en operación, con frecuencia alejadas de entre sí, por el espacio de distribución de las áreas de trabajo. Por ejemplo, una compañía con muchas fábricas puede tener un computadora en cada localidad para llevar el control de los inventarios, vigilar la productividad y pagar la nómina local. Inicialmente, cada una de estas computadoras puede haber trabajado aislada de otras, pero en algún momento la gerencia decidió conectarlas para extraer y correlacionar información acerca de toda la compañía.

En términos generales la cuestión importante es compartir los recursos y la meta es hacer que todos los programas, los equipos y especialmente los datos, estén disponibles para cualquier usuario en la red, sin importar la localización física de los recursos. En otras palabras, el hecho de que algún usuario este a cualquier distancia de sus datos, no debería impedirle usarlos como si no fueran locales.

PROPÓSITOS DE LA RED

Entre los propósitos más importantes de la red encontramos los siguientes:

- Acceso a información remota: esto es que cualquiera de las computadoras que estén conectadas a la red, podrá tener acceso a los datos que se encuentren en la misma, así aunque estos se encuentren en lugares alejados entre si, pero sí se encuentran en la red esto podrá llevarse acabo

- Comunicación de persona a persona: esto quiere decir que las personas se pueden comunicar y compartir información en archivos entre sí, siempre y cuando se encuentren conectadas a la red

- Entretenimiento interactivo: esto quiere decir que las personas que se encuentran conectadas a la red pueden tener una interacción entre ellas sin tener la necesidad de encontrarse en lugares cercanos, sino estando en lugares alejados uno del otro.

DIFERENCIA ENTRE SERVIDORES Y CLIENTES

La computadora de la red que tiene unidades de disco, la impresora o cualquier otro recurso que se comparta con otras computadoras de la misma red, se llama servidor. Cualquier computadora que no sea un servidor será llamado cliente (algunas veces es llamado también estación de trabajo). Hay únicamente dos tipos de computadoras en una red: servidores y clientes.

Usualmente, las computadoras más poderosas y más caras en una red son los servidores. Esto tiene sentido por cuanto a sus recursos, que son compartidos por todos los usuarios de la red. Las computadoras más baratas y menos poderosas son los clientes: son los equipos usados por los usuarios individuales en su trabajo cotidiano. Debido a que los recursos de los clientes no tienen que ser compartidos, (nodos) no tienen que ser tan sofisticados y por ende, mas caros.

Esto nos beneficia enormemente ya que nos ahorra tiempo de espera, compartir archivos, programas, recursos y sobre todo que la información esta disponible al momento que se requiere y hace que se acorten distancias y por medio de estas nos permite tener un buen control de trabajo, motivo por el cual se decidió conectar todos los equipos para extraer y correlacionar información. En términos generales la cuestión es compartir los recursos y la meta es hacer que todos los programas, el equipo y especialmente los datos estén disponibles para cualquier usuario en la red, sin importar la localización física de los equipos y de los usuarios, dicho en otras palabras el hecho de que algún usuario este alejado de su zona de trabajo no evita que pueda tener acceso a su información desde otro equipo de cómputo.

Los talleres La Paz, es un área propiamente de mantenimiento a trenes pero de la cual es necesario también llevar controles, estadísticas, informes para un buen mantenimiento y procesamiento de la información y ver de esta forma como van evolucionando las fallas, esto por medio de computadoras para la agilización de trabajos, tener controles actualizados, datos confiables y veraces, al mismo tiempo tratar de ahorrar tiempo a la medida de lo posible por lo cual ser realizó un planteamiento, el cual consistía en una RED INFORMÁTICA INTERNA, la cual nos permitiría agilizar la pronta solución de problemas, utilizando los recursos presentes, llámese computadoras, impresoras, etc. Para esto se dispone de un servidor y varias estaciones de trabajo ubicadas en puntos estratégicos del taller.

La Red informática que se pensó instalar en los Talleres La Paz y que actualmente ya esta funcionando se hizo considerando los beneficios que esto traería a corto, mediano y largo plazo en cuanto a su funcionalidad tomando en cuenta; cantidad de equipos de cómputo disponibles; se hizo pensando en que la red Cliente-Servidor traería mejores resultados en un futuro ya que se podrán incrementar más estaciones de trabajo y que la topología empleada proporcione el máximo rendimiento en condiciones críticas de trabajo.

Se determinó la necesidad de compartir bases de datos y tener la información que se genera en diversas áreas, y además de que se trabajará en un ambiente distribuido compartiendo y/o haciendo uso de los recursos disponibles.

En la parte de seguridad: se debe considerar que gran parte de la información es de naturaleza confidencial, y una red cliente servidor puede cumplir mejor este objetivo, por lo tanto se pueden compartir estos con otras áreas. con toda la certeza de poder establecer un servidor de datos seguro, que realice estas funciones.

Después de un análisis previo se opto por tomar la Topología Tipo Estrella la cual tiene por sí misma varias ventajas, una de ellas es que en este tipo de red todas las estaciones de trabajo están conectadas a un concentrador (hub) y en efecto cada nodo tiene una conexión independiente de las otras estaciones de trabajo de tal manera que una ruptura del cable o una falla en otra estación de trabajo no afectará a las demás.

Otra de las ventajas es que al instalar una red con la topología de estrella, se esta previniendo uno de los principales problemas en la transmisión de datos (una colisión) ya que cada estación de trabajo tiene un cable que se encuentra conectado a un puerto del concentrador (hub) por el cual envía la información y la recibe, para esto se decidió utilizar cable UTP de nivel 5 de par trenzado, el cual es el recomendado para este tipo de redes, además de que su velocidad puede variar de 10 a 100 Mb/s., y este es lo que en realidad conecta a las estaciones de trabajo entre sí.

También fue necesario colocar y configurar tarjetas de interfaz de red, ya que dentro de una estación de trabajo necesita una tarjeta de red compuesta de circuitos electrónicos llamada tarjeta de interfaz de red y su conexión es a través de un puerto tipo PCI o ISA, además de configurar los protocolos de comunicación de red, ya que estos sirven para la transmisión de datos y esto conlleva una serie que va desde el nivel físico hasta la presentación de la información en un formato determinado, aunque todos ellos son fundamentales y tienen un enlace encargado de la comunicación y esta comunicación se puede dividir en tres fases:

- Establecimiento de la comunicación: Esta consiste básicamente en la interconexión de dos o más computadoras los cuales requieren comunicación.
- Transferencia de la información: Se establece desde que una estación de trabajo solicita una serie de datos los cuales se convierten en información.
- Terminación de la comunicación: Se finaliza la comunicación al momento de que la estación de trabajo receptora recibe la información o se apague el equipo, y con esto podemos dar por concluida una fase de comunicación en red.

Sistemas operativos de redes

Es un sistema operativo que simula un ambiente multiusuario, en otras palabras, finge que todas las estaciones de trabajo dependen totalmente de él, aunque no es así.

En un sistema operativo en red, en el que los usuarios tienen conocimiento de la existencia de múltiples computadoras y pueden ingresar en maquinas remotas y ejecutar archivos de una maquina a otra. Cada maquina ejecuta su sistema operativo local y tiene un usuario propio (ó usuarios).

Existen varios Sistemas Operativos de Red, entre los que destacan los siguientes:

- NETWARE. El sistema operativo para redes de Novel en su más reciente versión cuenta con varios refinamientos orientados a facilitar la vida del administrador de sistemas, sobre todo en ambientes grandes con múltiples servidores. Cuenta con soporte para DOS, Windows, OS/2 y cliente Mac. es expandible a cliente-servidor, trabaja perfectamente en entornos pequeños con un solo servidor para toda la red o entornos grandes con varios servidores y conexiones a múltiples plataformas.

- WINDOWS 95/98/NT/Me. Este sistema operativo ofrece soporte automático para redes IPX/SPX, NetBEUI y TCP/IP. Brinda los servicios de WAN, compartir un módem como servidor de fax y correo electrónico.

- WINDOWS NT. Es un sistema operativo capaz de correr muchas aplicaciones de Windows. Escrito completamente en código de 32 bits, es un servidor de aplicaciones.

- UNIX. Es un sistema operativo robusto, con miles de aplicaciones desarrolladas, interfases de texto y gráficas.

- NEXT STEP. Es un UNIX gráfico orientado a objetos con muchas opciones de conectividad. Puede trabajar igualmente en entornos orientados a servidor de aplicaciones punto a punto.

Arquitectura cliente / servidor

Cliente-Servidor significa, a grandes rasgos, que algunas computadoras de la red actuaran como servidores de algún recurso (archivos, impresión, faxes, correo, bases de datos, etc.) para que puedan utilizarlos otras computadoras que se denominan clientes.

Este modelo de operación disminuye el tráfico en la red, facilita la coordinación de esfuerzos y centraliza operaciones críticas, de esta forma si se hace imperativa a la necesidad de mayor poder de cómputo, no es necesario elevar el nivel de todas las estaciones de la red, sino solo de mejorar el rendimiento de los servidores de aplicaciones implicados, generalmente a un costo menor y con mejores resultados.

Las necesidades actuales de cualquier organización exigen entornos de trabajo donde la información sea utilizada solo por la gente precisa y en lugar adecuado para ello, es que trabajar en red proporciona grandes beneficios, como compartir de forma controlada, recursos como impresoras o archivos o aplicaciones en disco duro.

Lenguajes de Cuarta Generación

Los lenguajes de cuarta generación son realmente algo más que lenguajes, en realidad son bases de programación, fueron creados para ayudar a satisfacer la necesidad de desarrollar software con mayor facilidad.

Los principales componentes de los lenguajes de cuarta generación son: Sistemas manejadores de Bases de Datos, diccionarios de datos, lenguaje no procedural, generador de reportes, generador de pantallas, código reutilizable, gráficas, procesador de palabras y editor de textos, herramientas para el modelar y analizar datos, programación de interfaces, desarrollo de bibliotecas de software, enlaces a otros DBMS.

El corazón de los lenguajes es el Sistema Manejador de Bases de Datos (DBMS) por que permite manipular (almacenar y recuperar) de manera eficiente los datos a un cuando sean texto, gráficas, voz o video; debido a su facilidad de uso, los lenguajes de cuarta generación son actualmente llamados: Aplicaciones orientadas al usuario final.

Prototipos

Es una metodología valiosa para identificar con rapidez las necesidades particulares de información del usuario. Consiste en una aplicación que trabaja, creada en forma rápida y económica por lo que mejora la efectividad total del esfuerzo del desarrollo para el beneficio del usuario, el analista y la organización en su conjunto.

El desarrollo de un prototipo de aplicación sigue un proceso iterativo que comienza con la identificación inicial de los requerimientos conocidos, con éstos se elabora el prototipo para posteriormente ser evaluado por los usuarios a medida que se evalúa, se van realizando modificaciones, es decir cada modificación requiere de una nueva evaluación por parte de los usuarios. Por medio de la iteración, el prototipo evoluciona hasta que llegue el momento de tomar la decisión de implantar el prototipo, transformándolo en un sistema completo o abandonar también, el proyecto por no cumplir con las necesidades reales de los usuarios.

Bases de Datos

Es un término informático aplicable generalmente en empresas, instituciones educativas, hospitales, bancos, etc., en donde se manejan grandes volúmenes de información, ya que esta es una herramienta que permite almacenar, clasificar y hacer uso de la información de manera más fácil y rápida que si se realizara en forma manual.

Una base de datos puede considerarse como una tabla que se compone de filas y columnas. Las filas en un archivo de base de datos se les conocen como registros y a las columnas se conocen como campos. O bien es un conjunto de datos organizados y almacenados en registros, en donde cada registro de la base de datos está compuesto por uno o más campos.

Tipos de Datos

Para definir el tipo de información que tendrán los campos, es necesario saber como se encuentran compuestos, esto es, por números y letras, etc. A esto le definimos como tipo de dato.

Los tipos de datos que pueden ser utilizados en una base de datos son:

Numéricos:	Aceptan exclusivamente dígitos.
Alfabéticos y carácter:	Aceptan algunos caracteres especiales, letras y dígitos.
Lógicos o boléanos:	Aceptan valores de falso y verdadero.
Memo:	Acepta texto en gran volumen

Tipos de Manejadores de Bases de Datos

Actualmente existen diversos manejadores de bases de datos, los cuales son un conjunto de programas que permiten hacer uso de estos para poder organizar y manipular la información; entre los manejadores de datos más comerciales tenemos los siguientes: SQL (el mas estándar a nivel mundial), INFORMIX, ORACLE, FOXPRO, ACCESS, etc.

MICROSOFT ACCESS

Es un sistema de administración de bases de datos relacionales para ambiente windows. El diseño de Access esta orientado a ofrecer una insuperable potencia de acceso a los datos, que se combina con la extrema facilidad de uso que permite windows.

Acces permite hacer bases de datos bien diseñadas, brinda un cómodo acceso a la información deseada dedicando menos tiempo a crear la base de datos y obteniendo resultados exactos en menos tiempo, las bases de datos Access están constituidas por diversos objetos: Tablas, consultas, formularios, informes, macros y módulos, estos objetos se enumeran en la ventana de la base de datos, donde se crean, se abren y se utilizan.

Si un equipo esta conectado en una red, varias personas podrían trabajar simultáneamente con una misma base de datos o archivo, mientras un usuario esta observando datos, otro puede estar modificando o eliminando esos mismos datos, igualmente mientras una persona esta utilizando un objeto de la base de datos, otra podría estar haciendo cambios en el diseño de dicho objeto.

La potencia real de una base de datos reside en su capacidad para mostrar los datos que se desean y en el orden en que se necesitan. Los datos de una consulta pueden proceder de una o varias tablas o archivos.

Desarrollo Orientado a Objetos

El Diseño Orientado a Objetos (DOO) crea un modelo del mundo real que pueden ser realizados en software. Los objetos proporcionan un mecanismo para representar el ámbito de información, mientras que las operaciones describen el procesamiento asociado con el ámbito de información.

El diseño orientado a los objetos representa un enfoque único para los ingenieros de software, proporcionándoles un método para romper barreras entre los datos y el procesamiento, además de mejorar la calidad del software.

VISUAL BASIC a 32 bits

Es un ambiente de programación orientado a eventos, que ha avanzado con cambios significativos desde su versión 1.0 hasta la 6.0 en menos de 6 años. Por ser un lenguaje de componentes, Visual Basic soporta su poder en lo que se denomina Controles, y que son añadidos del lenguaje "C", creados para realizar tareas que en otro código, podrían llevarse varias líneas de programación. Entre sus ventajas destaca el ser un ambiente de desarrollo autónomo.

El editor permite fijar controles en el área de desarrollo para evitar manipular accidentalmente su posicion, de igual manera se puede personalizar por completo el editor con el tipo de letra, tamaño y colores que se elijan. El lenguaje opera con colecciones de controles, así como con procedimientos de propiedades.

TECNOLOGÍA DE COMUNICACIÓN DE DATOS

Una red es un grupo de equipos conectados entre sí o a un servidor central, de manera que puedan compartir recursos, tales como documentos e impresoras, la conexión a una red, puede cambiar métodos de trabajo:

- Para utilizar programas y documentos de otros equipos sin necesidad de tener que utilizar discos.
- Poder imprimir documentos en una impresora conectada en otro equipo.
- Usar un fax módem de otro equipo como si estuviese conectado en cualquiera de toda la red.
- También enviar y recibir mensajes a través del correo electrónico, así como conectarse al equipo de su oficina desde su hogar.

Entre otras ventajas se encuentran las siguientes:

- Compartir información y recursos
- Ahorro en tiempos de trabajo
- Actualización inmediata de la información
- Máximo aprovechamiento de los recursos
- Evita duplicidad de trabajo y por lo tanto pérdida de tiempo
- Administración de información fácil y segura.
- Obtención de información en el momento oportuno
- Permite reducir cargas de trabajo

Tipos de Redes

Las cuatro grandes divisiones entre las redes de computadoras, se refieren al área donde están ubicadas las terminales y servidor en la red, estás son:

- Redes de Área Local (LAN).- Son las más comunes, como las de oficinas en un solo edificio, en tiendas o fábricas. Todos los recursos están a cargo del mismo servidor en una misma área.
- Redes de Área Abierta (WAN).- Esta red es la conexión de varias redes locales que se encuentran cercanas, de las cuales cada una tiene su propio servidor.
- Redes de Área Metropolitana (MAN).- Es la unión de varias redes a nivel estatal, en la cual cada red esta alejada considerablemente.
- Redes de Área Global (GAN)- Estas redes están conectadas a nivel internacional (enlaza varios puntos de gran cantidad de países), por lo que su tamaño es inmenso, un ejemplo claro y común es el Internet.

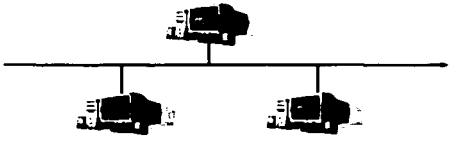
Topología de Redes

El concepto de topología es el que define la forma es que están interconectadas las estaciones de trabajo en la red. Existen cuatro tipos básicos de topología para red, BUS, ESTRELLA, ANILLO y ANILLO MODIFICADO.

Topología de Bus Lineal

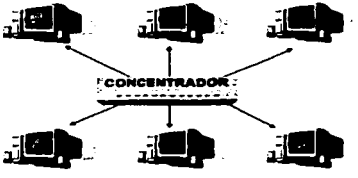
En la topología de Bus, todas las computadoras están conectadas a un mismo canal de comunicación y cualquier mensaje de red llega a todas las maquinas al mismo tiempo. El sistema operativo de red es el encargado de decidir quien debe responder al mensaje.

Su principal problema es que cuando hay muchas estaciones conectadas el rendimiento de la red desciende en forma notable, su representación gráfica es como a continuación se muestra.



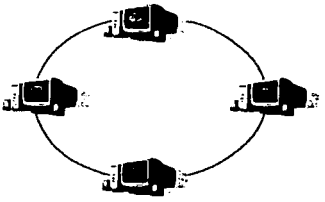
Topología de Estrella

La topología de Estrella se basa en unir todas las estacionas en un solo punto (máquina central). La principal ventaja que ofrece esta topología es que disminuye considerablemente el tráfico en la red, como se muestra en la siguiente figura.



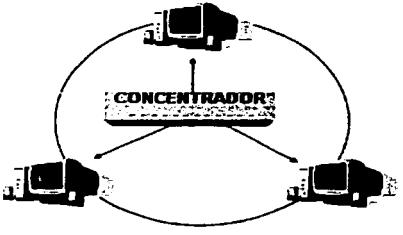
Topología de Anillo

En esta topología, las computadoras están conectadas de manera tal que den el aspecto de un círculo o anillo, como se muestra en la siguiente figura.



Topología de Anillo Modificado

En este tipo de topología, las terminales o las computadoras están conectadas a un concentrador, como se muestra en la siguiente figura.



Protocolo

Asociados a la topología, se encuentran los protocolos de comunicación de redes. Es decir, el conjunto de reglas que permiten a dos puntos de la red comunicarse entre sí. Estas reglas abarcan la construcción de mensajes completos con base en paquetes recibidos, identificar quien envía un mensaje y hacia quien va dirigido y la corrección de errores de transmisión.

Los protocolos mas populares son TCP/IP usado por UNIX y la base de todo Internet, IPX/SPX definido por Novell con su producto Net Ware, Apple Talk que es el estándar de Mac y SMB que es usado por Windows para trabajo en grupos y otros productos de Microsoft.

Los protocolos más comúnmente utilizados son:

- TCP/IP
- FAST ETHERNET 10/100

ORGANIGRAMA GENERAL DEL TALLER LA PAZ

A continuación se presenta un organigrama del Departamento para ver la distribución del personal y las áreas que conforman los Talleres la Paz, y de las cuales podemos describirlas

MANTENIMIENTO MENOR; Se encarga de las funciones del mantenimiento de los trenes, llámese bogles, cajas, averías, electrónica, así como las actividades correctivas, preventivas, cíclicas y sistemáticas, de todos los equipos que componen el tren

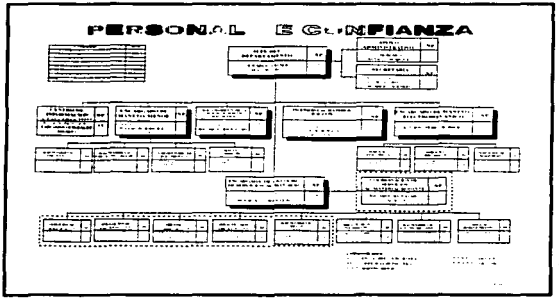
MANTENIMIENTO ELECTROMECÁNICO: Se encarga básicamente de tener todos los equipos electromecánicos funcionando en óptimas condiciones de operación, así, como de atender acciones imprevistas que se presente, ya que se encuentra dividida en mecánica, maquinado y eléctrica.

COORDINACIÓN DE SERVICIOS; Es el enlace con las otras áreas del departamento; es decir, con mantenimiento electromecánico, Mantenimiento Menor, Ingeniería; CiTa, además de reportar directamente a la jefatura del Departamento y otras Gerencias a las cuales se les reportan las actividades realizadas en el taller, además de atender programaciones anuales como son; Metas del Departamento, Recursos Humanos, Plantilla, Tiempo Extra, Vacaciones, procedimientos administrativos entre otros.

CITA: Esta área labora los 365 días del año, las 24 hrs., del día, en ella se reportan todos los incidentes que ocurren en la línea y se encargan de canalizarlas al área correspondiente y dar una solución inmediata a la problemática que se presente, en horarios en los que ya no están disponibles las demás áreas.

INGENIERÍA : Su función es la de tomar las actividades que como su nombre lo indica corresponden a la ingeniería, además de llevar seguimientos del aseguramiento al material rodante y a los trenes Modelo FM-95A.

MANTENIMIENTO MAYOR: L a finalidad de esta área es analizar y coordinar las actividades propias para el segundo Mantenimiento Mayor en la línea A.



DIAGNÓSTICO DE LOS RECURSOS DE LA UNIDAD INFORMÁTICA

Uno de los puntos más importantes en todo el desarrollo del proyecto es la seguridad informática, y se vuelve aún más relevante cuando se trata de utilizar la información, con la cual se alimentan los equipos de la red, para los diferentes procesos de trabajo necesarios para el mantenimiento, conservación y administración de los recursos actuales.

Debido a la importancia de la que representa la estructura en varios niveles de seguridad, desde un nivel externo vía red, hasta diversos niveles de seguridad internos en cada uno de los equipos correspondientes, analizaremos la importancia de accesos que tengan los equipos y ponerles los candados de seguridad que requieran dependiendo de la información que los usuarios utilicen y procesen, así mismo las restricciones que tienen los usuarios en el manejo de la información, de acuerdo al nivel de seguridad asignado.

SEGURIDAD A NIVEL RED

El primer candado de seguridad se da en el momento de encender el equipo (Estación de trabajo) con la solicitud del pasword de encendido, y posteriormente al cargarse el sistema operativo el pasword de entrada, el cual es un servidor dedicado posteriormente y toda vez que el sistema estará instalado en una red también será necesario contar con un "login" (entrada en la red) y un pasWord para acceder al servidor, una vez dentro de la red, se verifica si el usuario pertenece al grupo de trabajo que tiene los derechos de acceso al servidor, ya que solo ese grupo de usuarios tiene derecho para entrar a ese servicio,

Respaldos de red.- adicionalmente ya dentro del directorio dependiendo del usuario; de esta forma un usuario podrá leer y escribir, sobre un archivo, borrar, modificar, tener control total, etc, de acuerdo a sus privilegios, en tanto que otros sólo podrán leer y escribir y algunos más estarán restringidos a utilizar los archivos de solo lectura (todo esto se encuentra en proceso de implementación).

RECURSOS INFORMÁTICOS ACTUALES

Es importante saber con que recursos se cuenta para analizar de manera más precisa y ver el estado en el que se encuentran distribuidos y al mismo tiempo conocer la capacidad, velocidad de procesamiento y espacio disponible en cada uno de los equipos y saber si en algún momento determinado es posible compartir recursos para hacer más eficiente el servicio de red y de esta manera lograr la optimización y agilización debida de la información con la seguridad que corresponda a cada proceso de trabajo.

HARDWARE

NODO	UBICACIÓN	COMPUTADORA	PROCESADOR	SISTEMA OPERATIV	MEMORIA RAM	DISCO DURO	IMPRESORA
SERVIDOR DE RED							
Net Servet			x86 Family 5 Model	win NT 4.00.1381	130.484 KB	2.6 GB	
JEFATURA DEL DEPARTAMENTO							
Jefatura del Departamento al Material Rodante Ferreo		Vectra VL	Pentium	Win. 98	40 MB	1.2 MB	0SKB050866 LASER JET 5
COORDINACIÓN DE SERVICIOS							
Coordinación de Servicios al material Rodante		Vectra VL2	486 DX	DOS 6.2 Win. 3.1	38 MB	257 MB	6211370398 EPSON FX 1170
		Vectra VL	Pentium	Win. 98	32MB	1.19GB	
		Comercial	Ciryx 586	DOS 6.2 Win. 3.1	32 MB	226MB	2024751 ATI MT 131/24 E
		COMPAQ	PENTIUM 4	Win 98	128MB	37.2 GB	USCL04247 LASER JET 1200
COORDINACION DE MANTENIMIENTO MENOR							
Coordinacion de Mantenimiento Menor		Vectra500	Pentium	Win. 98	32 MB	4 GB	
Coordinacion de Mantenimiento Menor		Comercial	Ciryx 586	Win 98	16.0 MB	32 MB	2004605 ATI MT 131-9
INGENIERIA DEL MATERIAL RODANTE							
Coordinacion de Mantenimiento Menor		Vectra VL	Pentium	Win 98	32 MB	4 GB	609A101470 LASER JET 5L
CENTRO DE INFORMACION A TALLERES							
Coordinación de Mantenimiento Menor (C.I.T.A)		Vectra VL	Pentium	Win 98	32 MB	523 MB	RS18442 CANON LBP-8II
COORDINACION DE MANTENIMIENTO ELECTROMECÁNICO							
Coordinación de Mantenimiento Electromecanico a Talleres		Vectra500	Pentium	Win 95	32 MB	808 MB	VSHB020667 LASER JET 5 MP

SOFTWARE (licencias disponibles)

- Windows NT
- Windows 3.11
- Windows 95
- Office 95 (Word, Power Point, Excel, Access)
- Windows XP
- Windows 98
- Office 97
- McAffe

INFRAESTRUCTURA EN REDES

Red LAN interconectada (con topología de Estrella, Protocolo Fast Ethernet 10/100

DIRECTORIO DE EQUIPOS EN LA RED
DOMINIO: La Paz

TALLER LA PAZ				
NOMBRE PC	**GRUPO DE TRABAJO**	**DIRECCION IP**	**No DE SERIE**	**No DE INVENTARIO**
SERVIDOR	**La_Paz**	100.100.100.31	MX70620001	152398
CORPAZO1	**Coordinación**	100.100.117.1	3431402998	138037
CORPAZO2		100.100.117.2	65157660	150316
CORPAZO3		100.100.117.3	MC-20403492	149663
CORPAZO4		100.100.117.4	PERSONAL	
CORPAZO5		100.100.117.5	141BM28GB976	172431
JEFLAPAZ		100.100.117.6	65157667	150318
AVEPAZ01	**Talleres**	100.100.118.1	MX63350	156674
AVEPAZ02		100.100.118.2	M241550	115825
INGPAZ01		100.100.118.3	MX7020011	150914
INGPAZ02		100.100.118.4	MZ41550	115825
JEFMEPAZ		100.100.118.5	MX70450167	150692
MAYORPAZ		100.100.118.6	MX63550371	156669
CITAPAZ		100.100.118.7	MX70350065	150854
ELECTPAZ		100.100.118.8	TW62710552	156680
ALMPAZ01	**Almacenes**	100.100.119.1	6X1AKGMZN16V	173329
ALMPAZ02		100.100.119.2	55652236	138375
IMPRESORA		100.100.120.1	USKB059866	149620

HUBS COMPLEJO LA PAZ				
No.	**MARCA**	**No. PUERTO**	**VELOCIDAD**	**INVENTARIO**
HUB1	**centreCOMFH708SW**	8	10M/100M	162619
HUB2	**centreCOMFH708SW**	8	10M/100M	162620
HUB3	**centreCOMFH708SW**	8	10M/100M	162682
HUB4	**centreCOMFH708SW**	8	10M/100M	162622

TABLA DE ASIGNACIONES

Es importante mencionar que en la tabla de asignaciones se manejan los archivos, programas e información con la que opera, así mismo el nivel de seguridad con el que esta debe operar para tener un mayor control, para ello a continuación se presenta una tabla indicando los niveles de seguridad.

Para un mayor control de la información se definirán los niveles de seguridad, el nivel de acceso se dará de acuerdo a las funciones y actividades de cada usuario. El administrador de la red puede realizar y tener la característica de ser el único que puede modificar y dar accesos a los usuarios o cualquier otro cambio que así considere conveniente (dar mantenimiento a la red) así como ser el único que puede asignar espacios de discos para respaldo, control de recursos y privilegios de usuario, etc.

NOMBRE DEL NODO	DIRECTORIOS COMPARTIDOS	NIVEL DE SEGURIDAD	PROGRAMA Y/O APLICACIONES COMPARTIDAS	EQUIPO CON RELACIONES	OBSERVACIONES
SERVIDOR	Público	Alto	Respaldo de todos los backup de las estaciones de trabajo	Todos	
CSMR	Público	Alto	Programas de trabajos de Mantenimiento Mayor	Todos	
CSMR2	Público	Medio	Averías	Misma área	Bases de datos
CSMR3	Público	Medio	Requisiciones, Ordenes de Servicio	Todos	Solicitud de los mismos para consulta o modificaciones
CSMR4	Público	Medio	Presupuesto	Todos	Documentos Varios
CSMR5	Público	Medio	Metas, Informe Mensual	Todos	
CSMR6	Público	Medio	AVERIAS	AVERÍAS	BASES DE DATOS
JEFATURA	Público	Alto	Información Confidencial	Todos	
ELECTROMEÁNICO	Público	Medio	Información General	Todos	
INGENIERIA	Público	Medio	Información General	Todos	
CITA	Público	Bajo	Directorio	Todos	Información General del Depto. Incidentes en la línea.
MENOR	Público	Medio	Información General	Todos	
AVERIAS		Medio	Consulta de Bases de Datos	Área técnica	

CONCLUSIÓN **CAPÍTULO I**

Como primer instancia fue importante definir la necesidad que tiene la Seguridad Informática, y de esta forma mostrar lo relevante que es en todos y cada uno de los aspectos de forma independiente, por otra parte el conjunto de todos nos da como complemento una seguridad integral, para ello era conveniente revisar las políticas de acción, estrategias y metodologías.

También ha sido importante el haberles dado una presentación del proyecto de Seguridad Informática a todo el personal involucrado y al Jefe de Departamento, en la cual se plantearán los beneficios que se lograrían al tener mayor colaboración y asimismo crear conciencia en el personal operativo y para ello se analizó por medio de un formato de trabajo denominado FODA; en el cual se plantean las Fortalezas, Amenazas, debilidades y oportunidades para obtener información valiosa y al mismo tiempo analizarla, obteniendo así grandes beneficios para su análisis, reduciendo con ello los tiempos de respuesta.

Por otro lado, se considero necesario mencionar algunos antecedentes informáticos, que dieron origen a los programas actualmente utilizados, y algunos conceptos breves acerca de redes como topologías, sistemas operativos, lenguajes de programación, utilerías entre otros; llevándonos con esto a conocer los recursos informáticos actuales con los que se cuenta.

Además; el uso de equipos informáticos ha propiciado que en algunas ocasiones la información se concentra en manos de unas cuantas personas, pero ahora se vuelve imprescindible poner mayor atención a los aspectos de seguridad visibles y así hacer una revaloración de un amplio número de aspectos que bien valen la pena considerarlos dentro de la seguridad.

En el siguiente capítulo se hablará a detalle de lo que es la Seguridad Informática, así como, los tipos de seguridad que ayudaran a complementar la propia seguridad en los Talleres la Paz del Sistema de Transporte Colectivo, a fin de lograr una mayor interrelacion.

Se mencionará como información general de la aplicación de otras normas de Seguridad existentes. Así mismo, se hablará de una matriz de riesgos que coadyuve durante el proceso de investigación de campo mediante encuestas, entrevistas, análisis y diseño para la resolución de problemáticas.

De esta misma manera, se dará una explicación general de cada uno de los tipos de seguridad que se manejaran durante todo el proceso, también se darán algunos ejemplos de cómo elaborar planes de contingencia ante diversas circunstancias planteadas.

CAPÍTULO II

PLANEACION

CAPÍTULO II.- PLANEACIÓN

En la actualidad, gran parte de la información que se genera en los Talleres la Paz, es por medio de los equipos informáticos, a través de los diversos sistemas, programas y aplicaciones desarrolladas en las instalaciones del Sistema del Transporte Colectivo – Metro -, de los cuales algunos son de tipo operativo, donde se registran las operaciones rutinarias o de apoyo a la administración, mediante el análisis de información que facilite la toma de decisiones.

En la medida que han ido aumentando las actividades, controles de trabajo necesarios y recursos en forma, conjunta y paralelamente se integran riesgos, cuyas causas son las debilidades implícitas o explícitas que por su propia naturaleza presentan dichos recursos o actividades.

La Seguridad Informática global en los Talleres la Paz del S.T.C.-Metro- se fundamentará en el estudio cuidadoso de los riesgos potenciales a los que esta sometida mediante el análisis de una matriz de riesgos, donde se consideran los factores de las amenazas a las que se encuentre sometido y el impacto que estas pueden causar cuando se presentan.

OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

La Seguridad Informática la podemos definir como "el conjunto de procedimientos y técnicas para evaluar y controlar un sistema informático con el fin de constatar si las actividades son correctas y de acuerdo a las normativas informáticas y generales prefijadas.

La Seguridad Informática comprende no sólo la evaluación de los equipos de computo, de un sistema o procedimiento específico, sino que además evalúa los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

Esta es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un óptimo nivel de seguridad. Además de evaluar la organización de centros de información existentes de hardware y software.

La Seguridad de los Sistemas de Información en la empresa, a través de la evaluación y control que realiza, tiene como objetivo fundamental mejorar la rentabilidad, la seguridad y eficacia del sistema mecanizado de información en que se sustenta.

Los aspectos relativos al control de la Seguridad de la Información tienen tres puntos básicos en la seguridad de los sistemas de información:

- Aspectos generales relativos a la seguridad. En este grupo de aspectos se consideran, entre otros: la seguridad operativa de los programas, seguridad en suministros y funciones auxiliares, atmósferas agresivas, agresiones y posibles sabotajes, seguridad física de las instalaciones, del personal informático, etc.

- Aspectos relativos a la confidencialidad y seguridad de la información. Estos aspectos se refieren a la protección del material, además de los soportes de la información, también al control de acceso a la propia información (a toda o a parte de ella, con la posibilidad de introducir modificaciones en la misma).

- Aspectos jurídicos y económicos relativos a la seguridad de la información. En este punto se tratara de analizar la adecuada aplicación del sistema de información en los Talleres la Paz en cuanto al derecho a la confidencialidad y el derecho a la información, y controlar cada vez más los posibles delitos informáticos. La propia dinámica de la tecnología de la información y a su cada vez más amplia aplicación en la empresa. En general, estos delitos pueden integrarse en dos grandes grupos: delitos contra el sistema informático y delitos cometidos por medio del sistema informático. En el primer grupo se insertan figuras delictivas tipificadas en cualquier código penal, como hurto, robo, revelación de secretos, etc., y otro conjunto de delitos que ya no es tan frecuente encontrar, al menos con carácter general, perfectamente tipificados, como el denominado "hurto de tiempo", destrucción de información, delitos contra la propiedad material e intelectual de los sistemas de información (en equipos, respaldos, cintas magnéticas, etc).

En el conjunto de delitos informáticos cometido por medio de sistemas informáticos, cabría señalar que siempre son de carácter doloso, manipulaciones fraudulentas de programas lógicos, informaciones contenidas en bases de datos, falsificaciones, estafas, etc.

TIPOS DE SEGURIDAD EN INFORMÁTICA

- ***Investigación científica y humanística.*** Se usa en las computadoras para la resolución de cálculos matemáticos, recuentos numéricos, etc. algunas de estas operaciones son:
  - Resolución de ecuaciones
  - Análisis de datos de medidas experimentales, y encuestas.
  - Análisis automáticos de textos

- ***Aplicaciones técnicas.*** Usar la computadora para facilitar diseños de ingeniería y de productos comerciales, trazado de planos, etc. Algunas de estas operaciones son:
  - Análisis y diseño de circuitos de computadora
  - Cálculo de estructuras en obras de ingeniería
  - Minería y análisis topográficos
  - Cartografía y sismografía, etc.

- ***Documentación e información.*** Es uno de los campos más importantes para la utilización de computadoras. Estas se usan para el almacenamiento de grandes cantidades de datos y la recuperación controlada de los mismos en bases de datos. Ejemplos de este campo de aplicación son:
  - Documentación científica y técnica
  - Archivos automatizados de bibliotecas
  - Bases de datos jurídicas, estados financieros y estadística de operaciones bancarias y bursátiles.

- ***Gestión administrativa***. Automatiza las funciones de gestión típicas de una empresa. Existen programas que realizan las siguientes actividades; por mencionar algunos de ellos:
  - Contabilidad
  - Facturación
  - Inventarios
  - Nóminas

- ***Inteligencia artificial.*** Las computadoras se programan de forma que emulen el comportamiento de la mente humana. Los programas responden como previsiblemente lo haría una persona inteligente, por mencionar algunas aplicaciones como:
  - Reconocimiento del lenguaje natural
  - Programas de juego complejos (ajedrez)

- ***Instrumentación y control.*** Instrumentación electrónica, electromedicina, robots industriales para el control de procesos en serie.

  - Otras aplicaciones. Otros campos de aplicación no vistos anteriormente: video-juegos, aplicaciones en el arte, procesamiento de imágenes y música.

POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS DE UNA SEGURIDAD INFORMÁTICA

Definir una política de seguridad de red significa elaborar procedimientos y planes que salvaguarden los recursos de la red contra perdida y daño. Uno de los enfoques posibles para elaborar dicha política es examinar lo siguiente:

- ¿Qué recursos se están tratando de proteger?
- ¿De quiénes es necesario proteger los recursos?
- ¿Qué tan posibles son las amenazas?
- ¿Qué tan importante es el recurso?
- ¿Qué medidas pueden implementarse para proteger los bienes de forma económica y oportuna?
- Examinar periódicamente la política de seguridad de red para ver si han cambiado los objetivos y las circunstancias de la operación de la red.

En la figura No. 1, se muestra una hoja de trabajo que va ayudar a canalizar las ideas conforme estos lineamientos.[1]

- La columna "Nodo" es un nombre de red de identificación interna de los recursos que van a ser protegidos.
- La columna "Nombre del recurso de red" es la descripción en lenguaje común de los recursos. La importancia del recurso puede estar en una escala numérica del 0 al 10, o en expresiones 'Vagas" de lenguaje natural como bajo, alto, medio, muy alto, etcétera.
- La columna "Tipo de usuario del que hay que proteger al recurso" puede tener designaciones como interno, externo, invitado o nombres de grupos como usuarios de contabilidad, asistentes corporativos, etc.
- La columna "Posibilidad de una amenaza' puede estar en una escala numérica del 0 al 10, o en expresiones 'Vagas" de lenguaje natural como baja, media, alta, muy alta, etc.
- La columna "Medidas que se implementarán para proteger el recurso de red" puede tener valores tales como 'permisos de sistema operativo" para archivos y directorios; pistas/alertas de seguridad' para servicios de red; "routers de selección" y "firewalls" para hosts y dispositivos para conectividad de red; y cualquier otra descripción del tipo de control de seguridad.

En general, el costo de proteger las redes de una amenaza debe ser menor que el de recuperación en caso de que se viera afectado por una amenaza de seguridad.

[1] (referencia: Seguridad de Sistemas, Universidad católica de salta)

No dudar en contar con la ayuda de otros con conocimientos especializados respecto de los bienes de la red y de las posibles amenazas en su contra. Es importante hacer que en el diseño de la política de seguridad participe la gente involucrada en el uso y desarrollo de aplicaciones dentro de las instituciones.

Para lograr que la política de seguridad se utilice adecuadamente es importante hacer que participen todas las áreas, teniendo su cooperación, apoyo y aceptación.

HOJA DE TRABAJO PARA DESARROLLAR UN PLANTEAMIENTO DE SEGURIDAD

RECURSOS DE LA FUENTE			TIPO DE USUARIO DEL QUE HAY QUE PROTEGER AL RECURSO	POSIBILIDAD DE AMENAZA	MEDIDAS QUE SE IMPLEMENTARAN PARA PROTEGER AL RECURSO DE LA RED
NODO	NOMBRE	IMPORTANCIA DEL RECURSO			
		BAJO MEDIO ALTO MUY ALTO	INTERNO EXTERNO INVITADO O NOMBRES DE GRUPO COMO USUARIOS DE CONTABILIDAD, ASISTENTES CORPORATIVOS, STC.	ESCALA DEL 0 AL 10 BAJO ALTO MEDIO MUY ALTO	PERMISOS DE S.O. PARA ARCHIVOS Y DIRECTORIOS, PISTAS/ALERTAS DE SEGURIDAD PARA SERVICIOS DE RED.

Fig. No. 1

POLÍTICA DE SEGURIDAD EN INFORMÁTICA

La política de Seguridad Informática formará parte de los lineamientos generales a desarrollarse en base a las directivas emanadas del área de Informática y parte del compromiso de ésta en su aplicación. En ella se establecerán con claridad y precisión las metas a alcanzar y las responsabilidades asignadas.

A continuación se mencionan cuatro ejes principales por los cuales se establecera esta política:

- Programa de seguridad general de la organización.
- Programa de seguridad Informática a implementar.
- Programa sobre temas específicos como contingencias, seguridad física, etc
- Programas específicos sobre sistemas informáticos de información determinada.

Estos ejes de desarrollo utilizaran la información con una óptima relación costo-beneficio permitiendo compartir la información y ayudar a aprovechar mejor los recursos destinados a la Tecnología Informática (TI) en todo su potencial.

Algunos de los elementos a tener en cuenta al momento de implementar una política de seguridad informática son, por ejemplo:

- Establecimiento de una función que lleve a cabo la administración del Programa de Seguridad Informática que sea reconocida por toda la organización.
- Estándares, Guías, etc. que respalden las medidas tomadas, etc.

Por último se analizarán con detalle las pautas a considerar para la evaluación del nivel de cobertura existente ante situaciones de desastres, la identificación en forma anticipada de los factores de riesgo y la planificación de las acciones a seguir.

EVALUACIÓN DE RIESGOS

En cuanto al desarrollo e implementación de los distintos Programas de Seguridad Informática, se hace imprescindible basarse en una adecuada administración de los riesgos.

Riesgo es toda contingencia que pueda tener un efecto adverso sobre la organización, a través de un impacto en las actividades y/o en sus sistemas de información.

La administración de riesgos comprende la determinación, el alcance y la metodología de evaluación de los mismos, la recopilación y el análisis de los datos, la selección de las medidas de seguridad pertinentes, etc.

La selección de las medidas de seguridad deberá incluir en todos los casos elementos de seguridad física (edificios, recursos, infraestructura) y de seguridad lógica (accesos no-autorizados a sistemas, controles de programación, etc.)

ESTÁNDARES PARA LA ADMINISTRACIÓN DE ACCESO A LA INFORMACIÓN

Los controles de acceso a la información constituyen uno de los parámetros más importantes a la hora de administrar seguridad. Con ellos determinamos quién puede acceder a qué datos, indicando a cada persona un tipo de acceso (perfil de usuario) específico.

Para este cometido se utilizan diferentes técnicas que se diferencian significativamente en términos de precisión, sofisticación y costos. Se utilizan por ejemplo, palabras claves, algoritmos, listas de controles de acceso, limitaciones por ubicación de la información, horarios, etc.

Una vez determinados los controles de accesos a la información, se hace imprescindible efectuar una eficiente administración de la seguridad, lo que implica la implementación, seguimiento, pruebas y modificaciones sobre los "perfiles" de los usuarios de los sistemas.

Este es uno de los puntos fundamentales a tener en cuenta para garantizar la seguridad y al mismo tiempo una correcta accesibilidad a la información, en todo proyecto informático que pretenda brindar información a diferentes niveles, garantizando la correcta toma de decisiones y accesibilidad a un amplio especto de usuarios.

Para ello es importante que se plantee en la organización, la necesidad de establecer estándares para la administración de seguridad de accesos. Con ello se garantizará un eficiente, seguro y al mismo tiempo, correcto uso de la Información.

NECESIDAD DE LA ELABORACIÓN DE PLANES DE CONTINGENCIA Y RECUPERACIÓN DE DESASTRES

En la medida que el uso de los sistemas de información se expande y más personas dependen de su continuidad operativa. Es importante contar con un adecuado plan de contingencia y recuperación que facilite superar situaciones no deseadas o previstas.

Esto que parece algo elemental o trivial, no lo es tanto a la hora de su implementación práctica. Estamos muy habituados a encontrarnos en situaciones donde grandes organizaciones encargadas de procesar volúmenes importantes de datos, recurren a diferentes formas de trabajo, no siempre hechos con criterios correctos para poder "actualizar" sus datos que, seguramente no cuentan con planes de contingencia eficientes.

Algunas veces, realizando un trámite nos encontramos con la molesta circunstancia que no podemos completarlo por "problemas del sistema". Para poder implementar un eficiente nivel de cobertura ante situaciones de desastres que podrán ser de mayor o menor importancia de acuerdo a las circunstancias se debe tener en cuenta una serie de pautas, como son:

- Identificación en forma preliminar de factores de riesgos ante situaciones de desastres.
- Planificación de acciones a seguir.
- Designación de responsables de la implementación del plan.
- Asegurar el correcto funcionamiento del plan.

MATRIZ DE RIESGOS (ANÁLISIS DE RIESGOS Y ÁREAS DE OPORTUNIDAD)

Es importante mencionar la importancia que tiene la matriz de riesgos para así poder determinar cuales son los principales factores que más afectan a la organización en cuestiones informáticas, y así poder realizar un análisis de seguimiento adecuado para reducir riesgos en la información, software y hardware y plantear causas y controles para los mismos.

Este método requiere de la capacidad analítica, juicio y experiencia del auditor, especialmente para el análisis de resultados.

Para lograr una buena evaluación de la situación actual, los controles, causas y riesgos identificados deben segregarse y clasificarse. La elaboración de matrices es una excelente herramienta para este fin. Para elaborar las matrices se utiliza un formato que incluya riesgos de una "X", función y los probables controles necesarios. Pueden prepararse una o más matrices por cada segmento en que se haya dividido la función informática y/o por cada punto de Seguridad.

Durante la elaboración de las matrices, debe tenerse presente que la determinación de la suficiencia de un control es subjetiva y deben analizarse a la luz de los costos que implicaría, el implantar controles adicionales en contraposición con las posibles consecuencias.

La suficiencia de un control se evalúa a la luz de dos conceptos que son el impacto y la magnitud. El primero se refiere a la repercusión o influencia importante sobre algún punto específico de la función informática que se esté estudiando, mientras que la magnitud, se refiere a la cantidad monetaria que implicaría la materialización de dicho riesgo.

Para poder evaluar la relación que existe entre los elementos de la matriz, se deben analizar independientemente empezando con las causas de riesgo, para ello se debe asumir que todas las causas de riesgos se encuentran presentes previendo los riesgos que pueden generar así como la magnitud de los mismos.

Una vez evaluadas las causas de riesgos, se procede a cuantificar los riesgos que resultarán de la ocurrencia de alguna o algunas causas de riesgo que carezcan de controles adecuados y posteriormente se evalúan los controles clave que deberán actuar efectivamente sobre cada una de las causas potenciales de riesgo.

PRESENTACIÓN DE ASPECTOS SUSCEPTIBLES A CONTEMPLAR

Al realizar el análisis de los elementos, independientemente se estudia su relación empezando por evaluar la cobertura de los controles con respecto a las causas de riesgo, para ello se identifican aquellas causas de riesgo sobre las cuales no parece haber controles suficientes; a continuación se procede a evaluar la influencia de los controles sobre las causas de riesgo y el riesgo latente, de esta manera se puede indicar el grado en el que un control específico influirá en una causa específica y la probabilidad de ocurrencia de las causas de riesgo y/o la magnitud del mismo.

Al momento de analizar los diferentes controles que afecten a estas causas, también se puede determinar si se encuentran implantados efectivamente en una situación particular. Un control que se considere altamente confiable sobre la causa específica deberá ser el adecuado, a estos controles Si no existe un control fuerte deberán estar presentes dos o más controles de fuerza moderada Aún cuando éstos son útiles, no son considerados suficientemente confiables por si solos. Si no existen suficientes controles fuertes o de fuerza moderada, deberá haber un gran número de controles útiles pero no especialmente efectivos. Las causas de riesgo que no alcanzarán las calificaciones de control antes descritas se consideran como controladas insuficientemente. Por último se estima la magnitud y/o impacto de los riesgos identificados. Esto implica el evaluar en términos monetarios, la consecuencia máxima probable que pudiera resultar de un riesgo particular.

ÁREAS SUSCEPTIBLES	ASPECTO A EVALUAR POR ÁREA	CLASIFICACIÓN DEL RIESGO		
		ALTO	MEDIO	BAJO
Administración de cambios y problemas en aplicaciones	Metodología de atención a usuarios Registro y solución de problemas Control de versiones Pruebas y liberación de aplicaciones	X		
Controles de Acceso Lógico	Administración de recursos Dispositivos e información de acuerdo a facultades y privilegios otorgados	X		
Seguridad Cliente/Servidor	Tecnología de seguridad utilizada en el hardware y software del servidor Enlaces internos y estaciones de trabajo	X		
Seguridad en Redes	Enlaces Concentradores Conmutadores Servidores	X		
Administración de la Seguridad	Organización, funciones y Responsabilidades Políticas, normas y planes Estrategias de seguridad y responsabilidad en el manejo de la información.	X		
Planes de Contingencia	Administración, Planes, Estrategia, Tecnologías, y Procedimientos y recuperación en caso de desastre		X	
Seguridad Física	Mecanismos de seguridad de protección de personal, inmueble y tecnología de la información contra intrusión y afectación del medio ambiente			X

REALIZO

Susana Flores Leal

VISTO BUENO

Ing. Gerardo. J. Chacón Cruz
Departamento de Servicios de Mantenimiento al Material Rodante Férreo

Al realizar esta tabla comparativa se determinan las área susceptibles en las cuales están determinados los riesgos, las cuales se definen en base a las debilidades encontradas al realizar el análisis preliminar en conjunto con usuarios y personal que se encuentra involucrado es estas actividades.

JUSTIFICACIÓN DE LAS ÁREAS

Las cuales dieron como resultado del análisis previamente realizado.

CIRCUNSTANCIA	RIESGO
• Virus informático en red y equipos locales	• Daño de archivos • Perdida de la información
• Falta de actualización de respaldos y en algunos casos inexistencia de estos	• Atraso en la información para cumplir con trabajos, en tiempo y forma.
• Falta de control en acceso físico de personal al área de cómputo • Perdida de privacidad y confidencialidad del paswword	• Mal uso de la información • Borrado y copiado de la información confidencial
• No existe segregación de funciones	• Dependencia hacia personal que maneja proyectos clave
• Inexistencia de planes de contingencia en caso de desastre	• Perdida de tiempo para iniciar actividades
• Falta de políticas de seguridad	• Seguimiento nulo o informal de proyectos
• Manipulación erróneo de equipos por desconocimiento	• Deterioro y pérdida de equipos o componentes
• Inexistencia de catalogo de Jerarquías en Red	• Acceso a recursos y programas no permitidos
• Carencia de procedimientos y control seguridad para la información	• Falta de sistema preventivos y correctivos

PLAN DE SEGURIDAD INFORMÁTICA

Un enfoque sistemático para desarrollar e implantar un sistema de información esta compuesto de una serie de etapas. Estas etapas comprenden las siguientes partes, y las cuales se podrían seguir como se representa en la fig. No. 2

- Encuesta
  - Plan de actividades.
  - Entrevista informal con los usuarios.
  - Creación y aplicación de cuestionarios a los usuarios de la red.
- Análisis
  - Selección y tabulación de los datos obtenidos.
  - Identificación de los problemas y necesidades.
  - Definir requerimientos.
  - Establecer posibles soluciones.
  - Elaboración del informe correspondiente.
- Diseño
  - Investigar posibles alternativas con respecto a la tecnología y software existentes en la empresa.
  - Evaluar y seleccionar alternativas.
  - Diseño detallado de la solución.

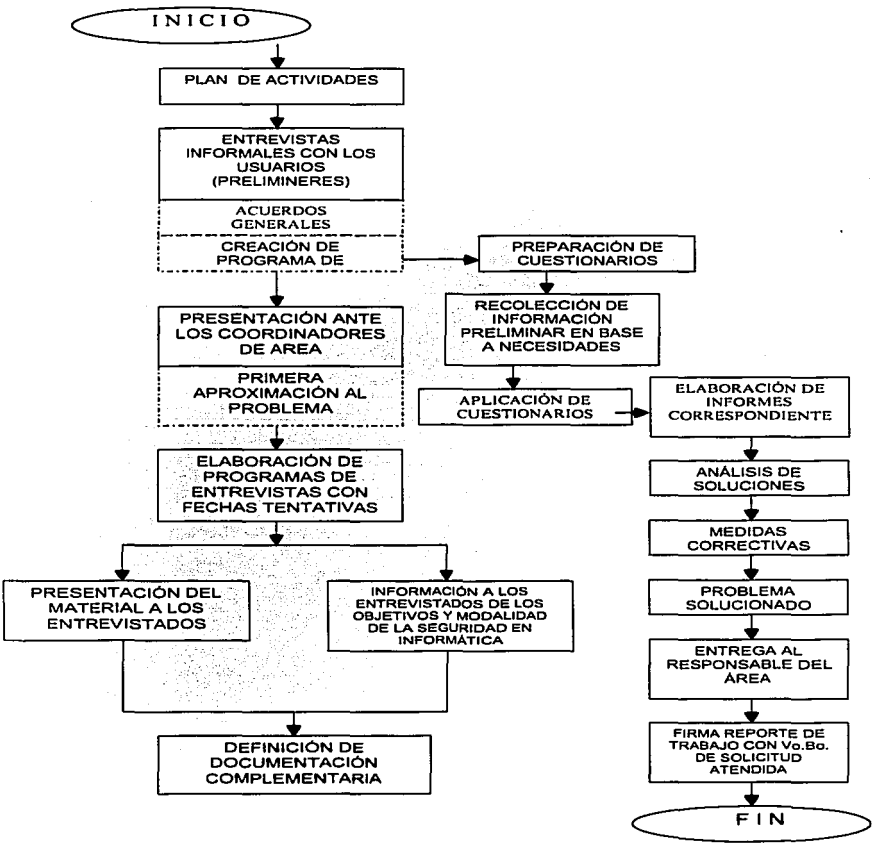


Fig. No. 2

CONSIDERACIONES PARA LA ELABORACIÓN DE PROGRAMAS DE SEGURIDAD

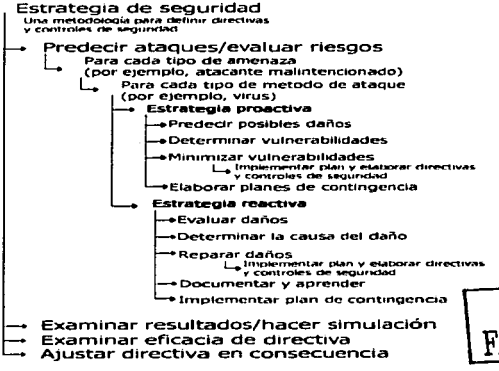
Para el desarrollo de los diversos programas de seguridad es necesario basarse en una adecuada administración de los riesgos.

La administración de los riesgos deberá entenderse como su identificación, evaluación y la posterior adopción de medidas que tiendan a minimizar y mantener los riesgos a un nivel aceptable para la organización. La administración de riesgos y su implementación comprende el desarrollo de una serie de actividades que serán objeto de tareas específicas de tecnología de seguridad informática.

Asimismo, es de gran importancia en la elaboración de programas de seguridad, tener especial consideración, el imprescindible equilibrio entre los costos y los beneficios a obtener con la puesta en marcha de los mismos. Es decir, el programa a implementarse permitirá establecer la existencia de una seguridad apropiada y costo razonable para cada instalación y/o sistema a instalar.

METODOLOGÍA PARA LA DEFINICIÓN DE ESTRATEGIAS DE SEGURIDAD

Para definir una estrategia de seguridad informática que se puede utilizar para implementar directivas y controles de seguridad con el objeto de aminorar los posibles ataques y amenazas. Los metodos se pueden utilizar en todos los tipos de ataques a sistemas, independientemente de que sean intencionados, no intencionados o desastres naturales, y, por consiguiente, se puedan volver a utilizar en distintos casos de ataque. La metodología se basa en los distintos tipos de amenazas, métodos de ataque y puntos vulnerables. El siguiente diagrama de flujo describe la metodología. [2]



[2] (este artículo proviene de Pilu.com http://www.pilu.com/core)

PREDECIR POSIBLES ATAQUES Y ANALIZAR RIESGOS

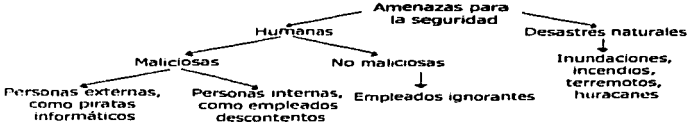
La metodología esquematizada en el diagrama de flujo es determinar los ataques que se pueden esperar y las formas de defenderse contra ellos. Es imposible estar preparado contra todos los ataques; por lo tanto, hay que prepararse para los que tiene más probabilidad de sufrir la organización. Siempre es mejor prevenir o aminorar los ataques, que reparar el daño que han causado.

Para mitigar los ataques es necesario conocer las distintas amenazas que ponen en peligro los sistemas, las técnicas correspondientes que se pueden utilizar para comprometer los controles de seguridad y los puntos vulnerables que existen en las directivas de seguridad. El conocimiento de estos tres elementos de los ataques, ayuda a predecir su aparición e incluso, su duración o ubicación. La predicción de los ataques trata de pronosticar su probabilidad, lo que depende del conocimiento de sus distintos aspectos. Los diferentes aspectos de un ataque se pueden mostrar en la siguiente ecuación:

Amenazas + Motivos + Herramientas y técnicas + Puntos vulnerables = Ataque

Para cada tipo de amenaza

Entre éstas se incluyen los agresores malintencionados, las amenazas no intencionadas y los desastres naturales. La siguiente ilustración clasifica las distintas amenazas a los sistemas. [3]



Amenazas como empleados ignorantes o descuidados, y los desastres naturales no implican motivos u objetivos; por lo tanto, no se utilizan métodos, herramientas o técnicas predeterminadas para iniciar los ataques. Casi todos estos ataques o infiltraciones en la seguridad se generan internamente; raras veces los va a iniciar alguien ajeno a la organización. Para estos tipos de amenazas, el personal de seguridad necesita implementar estrategias proactivas o reactivas siguiendo las instrucciones del diagrama.

Para cada tipo de método de ataque

Para iniciar un ataque, se necesita un método, una herramienta o una técnica para explotar los distintos puntos vulnerables de los sistemas, de las directivas de seguridad y de los controles. Los agresores pueden utilizar varios métodos para iniciar el mismo ataque. Por lo tanto, la estrategia defensiva debe personalizarse para cada tipo de método utilizado en cada tipo de amenaza. Una vez mas, es importante que los profesionales de la seguridad estén al día en los diferentes métodos, herramientas y técnicas que utilizan los agresores. A Continuación se muestras una lista breve de estas técnicas:

[3] (este articulo proviene de Pilu.com http://www.pilu.com/core)

- Ataques de denegación de servicio
- Ataques de invasión
- Ingeniería social
- Virus
- Gusanos
- Caballos de Troya
- Modificación de paquetes
- Repetición de paquetes
- Adivinación de contraseñas
- Intercepción de correo electrónico

Determinar el daño posible que puede causar un ataque

Los daños posibles pueden oscilar entre pequeños fallos del equipo y la pérdida, catastrófica, de los datos. El daño causado al sistema dependerá del tipo de ataque. Si es posible, se utilizara un entorno de prueba o de laboratorio para clarificar los daños que provocan los diferentes tipos de ataques. Ello permitirá al personal de seguridad ver el daño físico que causan los ataques experimentales, sin embargo es conveniente considerar que no todos los ataques causan el mismo daño.

Éstos son algunos ejemplos de las pruebas que se ejecutaron para determinar el grado y causa del ataque.

- Simulación de un ataque con virus a través de correo electrónico en el sistema y ver el daño que ha provocado y cómo recuperarse de la situación,

  Solución: Para lo cual se tuvo que vacunar cada uno de los equipos, para determinar cuantos equipos se encontraban infectados, así como los archivos, detectándose en un 30%, solucionando afortunadamente sin mayores problemas siendo que no era un virus muy arraigado, debido a la actualización de antivirus en varios equipos de la red.

- Utilizar la ingeniería social para adquirir un nombre de usuario y una contraseña de algún empleado ingenuo y observar cómo se comporta.

  Solución: En esta situación en particular como no existen usuarios experimentados o de alto nivel informático, se dio el caso de que ni siquiera se entero el usuario, de que había una intromisión en su equipo.

- Simulación de un ataque de virus dañino. Se estimó el tiempo necesario para recuperar un equipo y multiplique ese tiempo por el número de equipos del sistema infectados para determinar el tiempo de inactividad y la pérdida de productividad.

  Solución: Esto proceso requirió aproximadamente de 2 horas, fingiendo ante el usuario que era un virus altamente peligroso y que además podría llegar a la perdida total de la información, creando con esto un sentido de responsabilidad ante el propio usuario y que estuviera al pendiente del control de los respaldos de su información. Si consideramos que existen 15 equipos en red, esto sería el equivalente a 30 hrs. de pérdida de trabajo, retraso en la actualización de la información, las consiguientes horas de trabajo turno/hombre.

- También es aconsejable implicar al equipo de respuesta a incidentes ya mencionado, ya que es más probable que un equipo, en lugar de una sola persona, consiga localizar todos los tipos distintos de daños que se han producido.

  Solución: Para esto se analizo mediante la utilización del formato FODA, y a su vez entrevistando a cada usuario para, ver más de cerca su problemática y resolverla lo mas pronto posible.

Puntos vulnerables o las debilidades que pueden explotar los ataques

Si se pueden descubrir los puntos vulnerables de un ataque específico, se pueden modificar las directivas y los controles de seguridad actuales o implementar otras nuevas para reducir estos puntos vulnerables. La determinación del tipo de ataque, amenaza y método facilita el descubrimiento de los puntos vulnerables existentes y esto se puede reconocer por medio de una prueba real.

DEFINICIÓN DE CADA UNO DE LOS TIPOS DE SEGURIDAD Y PUNTOS A ANALIZAR

SEGURIDAD FÍSICA DE LAS INSTALACIONES Y EQUIPOS

Incluye los mecanismos de seguridad de protección de personal, inmueble y tecnología de información contra intrusión, afectación del medio ambiente, incendio y desastre y cortes de líneas de transmisión.

ADMINISTRACIÓN DE CAMBIOS Y PROBLEMAS DE APLICACIONES

Los elementos a tener en cuenta en seguridad referentes a la administración del Personal encargado de operar los Sistemas de Información y de los usuarios en general están relacionados con las interacciones de las personas, los equipos informáticos y las autorizaciones que cada uno necesita para llevar a cabo su trabajo. Para ello podemos mencionar algunos puntos que consideramos los fundamentales para esta tarea:

- Organización del personal.
- Administración de usuarios
- Permisos de accesos del personal contratado.
- Accesos públicos.

Este último punto, es de gran importancia, en todo sistema que lo requiera, para la determinación de la seguridad, pues requiere de la aplicación de medidas específicas, ya que, por razones lógicas, se incrementa notablemente el riesgo y se dificulta la administración.

CONTROLES DE SEGURIDAD DE ACCESO LÓGICO

Para ello es importante la administración y autentificación de usuarios, dispositivos e información de acuerdo a las facultades y privilegios otorgados por los controladores de la información para que cada usuario pueda acceder a los recursos a que este autorizado y realizar solo las funciones permitidas, lectura, variación, ejecución, borrado, copia y quedando las pistas necesarias para control y seguridad tanto de acceso producidas al menos a los recursos mas críticos como los intentos en determinados casos.

SEGURIDAD EN DATOS (Cliente/Servidor)

Involucra la tecnología de seguridad utilizada en el hardware y software de los servidores, enlaces internos y estaciones de trabajo.

El acceso global a la información que trajo el advenimiento de la tecnología de Internet, ha hecho que el problema de seguridad de la información se acrecentara de manera alarmante.

En función de esta realidad, se deben extremar los requerimientos de seguridad en todos los elementos que configuren el sistema de información.

El Sistema de base de datos que decidamos utilizar en una aplicación determinada, deberá ser valorado, fundamentalmente por la seguridad que brinde a la información.

Existen, actualmente, criterios de evaluación de seguridad, con validez internacional, que permiten clasificar cada sistema de base de datos en distintas categorías de acuerdo a la valoración, que de él hagan grupos de expertos en el tema.

Asimismo se estudia con sumo cuidado las facilidades que el sistema de base de datos ofrece, qué tipo de información genera, con qué facilidad se pueden definir opciones, y que equipos son más susceptibles de que ocurran errores considerables, así como la frecuencia en que ocurren etc.

Un aspecto que merece atención es el control de acceso que posea, la posibilidad de definición de perfiles y grupos del mismo.

Si el procesamiento es distribuido será objeto de nuestra atención el procesamiento y replicación segura, así como también todo mecanismo que garantice la integridad de LOS DATOS en forma automática.

SEGURIDAD DE COMUNICACIONES

Se considera la red de comunicaciones, con sus enlaces, topologías, protección de antivirus en sistemas aislados, conmutadores, concentradores, ruteadores y servidores.

En el Procesamiento en Redes, la distribución de responsabilidades en las distintas etapas de las tareas específicas del mismo, hace que cualquier medida de Seguridad a implementarse, incluyendo por supuesto, la implementación de Planes de Contingencias se incremente en complejidad y en la consideración de recursos locales y remotos.

Existen para estos casos un conjunto de medidas que se consideraran, las cuales varían en función de los inconvenientes previstos y analizados.

Es muy necesario en estos casos contar con programas (software específico) que efectúen el análisis de las redes y sus recursos, para poder detectar anomalías en el funcionamiento de las mismas, se considera necesaria la inclusión de control de accesos a directorios, archivos, registros, control contra-robo de datos, e introducción de software ajeno a la organización con el riesgo de incorporación de virus a la red que pueden traer complicaciones graves.

Una de las condiciones necesarias, en general para todo sistema de seguridad, es garantizar la participación y compromiso de la alta dirección, este compromiso, no sólo deberá asegurar el apoyo necesario sino establecer claramente los objetivos y asegurar el cumplimiento de la planificación.

PLANES DE SEGURIDAD EN CONTINUIDAD DE LAS OPERACIONES

Esta etapa detalla la administración, planes, estrategias y procedimientos de recuperación en caso de ocurrir una contingencia, para los cuales casi todos tienen puntos de enlace y partes comunes, control de acceso, cifrado con comunicaciones y soportes, datos con soportes y con comunicaciones, y otros puntos de seguridad existentes.

ADMINISTRACIÓN DE LA SEGURIDAD

- Esta contiene la organización, funciones, responsabilidades, políticas, normas y planes así como las estrategias de seguridad informática, responsabilidades en el manejo de la información (clasificación, acceso y uso).
- Uno de los objetivos quizá, de mayor importancia, en todo proyecto informático es poner a disposición de la mayor cantidad de personas, la información procesada será factible, sólo si se planifican desde el comienzo del diseño de sistemas medidas que garanticen un acceso ágil y seguro a la información clasificada como pública.
- Adoptar nuevas medidas de seguridad a un sistema, luego de que ha ocurrido alguna violación o falla cuando éste ya ha sido implementado (como sucede a diario en la mayoría de los casos) puede traer consecuencias no deseables y provocar una mala relación costo-efectividad de los controles.
- Para que esto no ocurra, desde las etapas preliminares del diseño, debemos cerciorarnos de que se tomen las medidas necesarias para implementar seguridad en todos y cada uno de los componentes del sistema, (bases de datos, redes de procesamiento, Internet, personal, equipamiento, etc.)
- El acceso público a la información clasificada como tal, es algo que en función de los recursos tecnológicos y de comunicaciones de los que disponemos hoy, no tendría que ser objeto de ningún tipo de limitaciones, sin embargo, si todo el entorno informático no está preparado para ese objetivo desde el punto de vista de seguridad, es muy difícil llevar adelante los procesos involucrados.

SEGURIDAD EN INTERNET

Agrupa el uso de tecnología en Internet e Intranet con sus mecanismos de protección (firewall y encriptación)

Nadie escapa de la formidable expansión que ha tenido en estos últimos años la "Red de Redes" o lo que comúnmente llamamos "Supercarretera de la Información" permitiendo el acceso de la información de todo tipo a todo el mundo a un costo considerablemente bajo. Además esta nueva tecnología realmente ha convertido el modo de comunicarse, relacionarse comercial, académica y profesionalmente, de una manera como nunca antes existió. Este formidable cambio, en tan poco tiempo, ha hecho que, tecnológicamente, aún no se hayan desarrollado los elementos de seguridad suficientes para garantizar una absoluta privacidad e integridad de los datos que viajan por la red.

No obstante, los expertos en seguridad informática han desarrollado sistemas que, bajo ciertas condiciones, y con determinados elementos, nos permiten la utilización de la Internet, con un grado de seguridad aceptable.

En esta primera etapa del desarrollo de seguridad en Internet, se ha comenzado ha trabajar con cuatro componentes fundamentales, que son:

Autenticación e identificación.- Técnica que nos permiten individualizar al autor de determinada acción.
Autorización.- Técnica que permite delimitar a qué información tienen acceso determinadas personas.
Integridad de datos.- Técnica que garantiza que los datos que viajan por la Internet lleguen intactos a su destino.
Privacidad de datos.- Técnica que determina quién puede leer la información una vez que salió del sistema de almacenamiento.

El grado de avance en estas tecnologías utilizando sistemas de "firewalls" físicos y lógicos como así también encriptación de datos nos permite, con un diseño apropiado. Utilizar esta tecnología como la interfase natural de comunicación en todos nuestros sistemas de información, permitiendo que de cualquier parte del mundo se pueda acceder a ellos con la seguridad necesaria.

ELABORAR PLANES DE CONTINGENCIA

Un plan de contingencia es un plan alternativo que debe desarrollarse en caso de que algún ataque penetre en el sistema y dañe los datos o cualquier otro activo, detenga las operaciones comerciales habituales y reste productividad. El plan se sigue, si el sistema no se puede restaurar a tiempo. Su objetivo final es mantener la disponibilidad, integridad y confidencialidad de los datos. Debe haber un plan para cada tipo de ataque y tipo de amenaza. Cada plan consta de un conjunto de pasos que se han de emprender en el caso de que un ataque logre traspasar las directivas de seguridad. El plan de contingencia debe:

- Determinar quién debe hacer qué, en qué momento y para que la organización siga funcionando.
- Ensayarse periódicamente para mantener al personal informado de los procedimientos en caso de contingencia.
- Abarcar la restauración de las copias de seguridad.
- Explicar la actualización del software antivirus.
- Abarcar el traspaso de la producción a otra ubicación o sitio.

Los siguientes puntos resaltan las distintas tareas que deben evaluarse para desarrollar un plan de contingencia:

- Evaluar las directivas y controles de seguridad de la organización para utilizar todas las oportunidades destinadas a reducir los puntos vulnerables. La evaluación debe tratar el plan y los procedimientos de emergencia actuales de la organización y su integración en el plan de contingencia.
- Evaluar los procedimientos actuales de respuesta ante emergencias y su efecto en el funcionamiento continuo de la organización.
- Desarrollar respuestas planeadas a ataques, integrarlas en el plan de contingencia y anotar hasta qué punto son adecuadas para limitar el daño y reducir el impacto del ataque en las operaciones de procesamiento.
- Evaluar procedimientos de copia de seguridad, que incluyan la documentación más reciente y pruebas de recuperación de desastres, para evaluar su adecuación e integrarlos en el plan de contingencia.
- Evaluar planes de recuperación de desastres para determinar su adecuación con el fin de proporcionar un entorno operativo temporal o bien a largo plazo. Los planes de recuperación de desastres deben incluir la prueba de los niveles de seguridad necesarios, con el fin de que el personal de seguridad pueda ver si siguen exigiendo la seguridad en todo el proceso de recuperación o en operaciones temporales y el traspaso de la organización otra vez a su sitio de procesamiento original o a un sitio nuevo.

Redactar un documento detallado que describa los distintos descubrimientos en las tareas anteriores, mismo que debe contener:

- Todos los casos para probar el plan de contingencia.
- El impacto de las dependencias y la ayuda planeada de fuera de la organización, y las dificultades que la obtención de los recursos esenciales tendrán en el plan.
- Una lista de prioridades observadas en las operaciones de recuperación y el fundamento para establecerlas.

Reducir los puntos vulnerables y debilidades que puede explotar un posible ataque.

La reducción de los puntos vulnerables y las debilidades del sistema de seguridad que se mencionan en la evaluación anterior es el primer paso para desarrollar directivas y controles de seguridad eficaces. Ésta es la compensación de la estrategia proactiva. Mediante la reducción de los puntos vulnerables, el personal de seguridad puede hacer disminuir tanto la probabilidad de un ataque como su eficacia, si se produce alguno. Debe haber un cuidadoso equilibrio entre los controles de seguridad y el acceso a la información. Los usuarios deben tener la mayor libertad posible para tener acceso a la información, pero con la seguridad de acceso debida.

Estrategia proactiva

La estrategia proactiva es un conjunto de pasos predefinidos que deben seguirse para evitar ataques antes de que ocurran. Entre estos pasos se incluye observar cómo podría afectar o dañar el sistema, y los puntos vulnerables que explota. Los conocimientos adquiridos en estas evaluaciones pueden ayudar a implementar las directivas de seguridad que controlarán o aminorarán los ataques. Éstos son los tres pasos de la estrategia proactiva:

- Determinar el daño que causará el ataque.
- Establecer los puntos vulnerables y las debilidades que explotará el ataque.
- Reducir los puntos vulnerables y las debilidades que se ha determinado en el sistema para ese tipo de ataque específico.

El seguimiento de estos pasos para analizar los distintos tipos de ataques tiene una ventaja adicional: comenzará a emerger un modelo, ya que en los diferentes factores se superponen para diferentes ataques. Este modelo puede ser útil al determinar las áreas de vulnerabilidad que plantean el mayor riesgo para la empresa. También es necesario tomar nota del costo que supone la pérdida de los datos frente al de la implementación de controles de seguridad. Las directivas y controles de seguridad no serán, en ningún caso, totalmente eficaces al eliminar los ataques. Éste es el motivo por el que es necesario desarrollar planes de recuperación y de contingencia en caso de que se quebranten los controles de seguridad.

Estrategia reactiva

La estrategia reactiva se implementa cuando ha fallado la estrategia proactiva y define los pasos que deben adoptarse después o durante un ataque. Ayuda a identificar el daño causado y los puntos vulnerables que se explotaron en el ataque, a determinar por qué tuvo lugar, a reparar el daño que causó y a implementar un plan de contingencia, si existe. Tanto la estrategia reactiva como la proactiva funcionan conjuntamente para desarrollar directivas y controles de seguridad con el fin de reducir los ataques y el daño que causan.

El equipo de respuesta a incidentes debe incluirse en los pasos adoptados durante o después del ataque para ayudar a evaluarlo, a documentar el evento y a aprender de él.

Evaluar el daño

Se deberá determinar el daño causado durante el ataque. Esto debe hacerse lo antes posible para que puedan comenzar las operaciones de restauración. Si no se puede evaluar el daño a tiempo, debe implementarse un plan de contingencia para que puedan proseguir las operaciones comerciales y la productividad normales.

Determinar la causa del daño

Para determinar la causa del daño, es necesario saber a qué recursos va dirigido el ataque y qué puntos vulnerables se explotaron para obtener acceso o perturbar los servicios. Revisar los registros del sistema, los registros de Seguridad y las pistas de Seguridad. Estas revisiones suelen ayudar a descubrir el lugar del sistema en el que se originó el ataque y qué otros recursos resultan afectados.

Reparar el daño

Es muy importante que el daño se repare lo antes posible para restaurar las operaciones normales y todos los datos perdidos durante el ataque. Los planes y procedimientos para la recuperación de desastres de la organización deben cubrir la estrategia de restauración. El equipo de respuesta a incidentes también debe poder controlar el proceso de restauración y recuperación, y ayudar en este último.

Documentar y aprender

Es importante documentar el ataque una vez que se ha producido. La documentación debe abarcar todos los aspectos que se conozcan del mismo, entre los que se incluyen el daño que ha causado (en hardware y software, pérdida de datos o pérdida de productividad), los puntos vulnerables y las debilidades que se explotaron durante el ataque, la cantidad de tiempo de producción perdido y los procedimientos tomados para reparar el daño. La documentación ayudará a modificar las estrategias proactivas para evitar ataques futuros o mermar los daños.

Revisar el resultado y hacer simulaciones

El segundo paso importante en la estrategia de seguridad es revisar los descubrimientos establecidos en el primer paso (predicción del ataque). Tras el ataque o tras defenderse de él, revisar los resultados con respecto al sistema. La revisión debe incluir la perdida de productividad, la pérdida de datos o de hardware, y el tiempo que se tarda en recuperarlos. Documentar el ataque y, si es posible, hacer un seguimiento del lugar en el que se originó, que métodos se utilizaron para iniciarlo y qué puntos vulnerables se explotaron.

Revisar la eficacia de las directivas

Si hay directivas para defenderse de un ataque que se ha producido, hay que revisar y comprobar su eficacia. Si no hay directivas, se deben redactar para aminorar o impedir ataques futuros.

Ajustar la directiva en consecuencia

Si la eficacia de la directiva no llega al estándar, hay que ajustarla en consecuencia. Las actualizaciones de las directivas debe realizarlas el personal directivo relevante, los responsables de seguridad, los administradores y el equipo de respuesta a incidentes. Todas las directivas deben seguir las reglas e instrucciones generales de la organización. Por ejemplo, el horario laboral puede ser de 9 a.m. a 6 p.m. Podría existir o crearse una directiva de seguridad que permita a los usuarios conectarse al sistema solamente durante este horario.

CONCLUSIONES CAPÍTULO II

Para llevar un buen control y tener el apoyo del personal, ha sido importante involucrarlos primeramente, para que apoyarán como parte fundamental en el planteamiento de riesgos existentes, siendo estos básicamente los que hacen que reduzca su eficiencia, aumentando el costo y la amenaza de pérdida de información o de recursos físicos, por ello era vital identificar riesgos para así ser analizados y evaluarlos, de esta forma; si no es posible eliminarlos definitivamente si reducir el impacto y la probabilidad de que ocurran.

Por ello, ha sido trascendente plantear los objetivos de Seguridad, mencionando:¿para qué sirven los tipos de seguridad que se llevan a cabo? para lograr la seguridad informática, planteando en primer instancia los recursos a proteger, ¿de quien? y ¿para que?, así como las posibles amenazas presentes y la importancia de los recursos, para en la medida de lo posible implementar medidas de seguridad para su protección.

En el siguiente capítulo se planteará una metodología de estudio, con la intención de tener un panorama más amplio de las funciones que abarca el Departamento en cuanto a informática se refiere, y las actividades que serán objeto de estudio, así como las técnicas y herramientas a ser utilizadas, implementando los formatos de cuestionarios a ser aplicados con cada uno de los usuarios de los Talleres la Paz y que hacen uso de la red interna.

CAPÍTULO III

IMPLEMENTACION

CAPÍTULO III.- IMPLEMENTACIÓN

Se compone de un conjunto de tareas estructuradas para que el proyecto de seguridad en informática se adapte a las necesidades. Las tareas realizadas deben cumplir con los estándares, políticas y procedimientos establecidos por las asociaciones profesionales, así como acatar lo establecido durante el desarrollo de seguridad.

PLAN Y METODOLOGÍA DE ACUERDO AL USUARIO (ENTENDIMIENTO DE LAS ACTIVIDADES QUE REALIZA Y LA FUNCIÓN

Para cumplir con los objetivos del presente proyecto se plantean las actividades en cada uno de los equipos de la red de tal manera que permita tener un panorama más claro y al mismo tiempo explotar de manera creciente los recursos informáticos.

Para satisfacer las necesidades reales de uso y explotación de los equipos de computo, trataremos de agrupar todas las actividades a fin de sacar el mayor beneficio de la organización actual de la información para lo cual se realizaran cuestionarios de una forma programada y en base a las necesidades de cada coordinación, considerando que cada día se vuelve mas necesaria la seguridad de la información, de los equipos y de todos los recursos con los que cuenta la empresa.

En esta etapa de implementación de información documental e informática se ha definido como objetivo principal integrar los sistemas y aplicaciones de tal forma que toda la información y recursos sea compartida a nivel departamento, así mismo que en cada usuario se cree una jerarquización de derechos y privilegios previniendo con esto que haya posibles alteraciones en la red particularizándola como el usuario de origen y auxiliar para los demás, hasta alcanzar un sistema integral.

En este estudio se ha contemplado una estructuración de trabajo integral que permita a los usuarios tener la capacidad de resolver y desarrollar cualquier actividad de forma ágil, eficiente considerando aquellos programas (software Institucional oficial autorizado) de uso más generalizado que permitan implementar una estructura generalizada y sencilla de aplicaciones dentro de un ambiente operativo sencillo, homogéneo e integrado que permita compartir información entre si, para evitar la dependencia hacia el personal calificado o responsable de la actividad de tal manera que todo el personal de los Talleres La Paz, cuente con los elementos necesarios para desarrollar sus actividades usando las computadoras, como herramientas de trabajo y de mayor productividad.

Cuestionario de diagnóstico actual
"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

Concepto	Descripción	Comentarios
Giro y Misión del negocio (Solicitar Organigrama) Transporte de pasajeros	Se encarga de brindar servicio a usuarios de L-A (La Paz -Pantitlán)	La informática dentro de los talleres se ha ido implementando poco a poco debido a la creciente necesidad y funcionalidad de la misma.
areas del negocio		
• Mantenimiento Menor	• Realización de los mantenimientos preventivos, correctivos, averías, bogies, cajas, electrónica.	
• Mantenimiento Electrico	• Mantener en buen estado los equipos electromecánicos.	
• Coordinación de Servicios	• Brinda apoyo informático, técnico administrativo a todo el Departamento.	Las areas existentes ayudan de gran manera en la solución a corrección de fallas.
• Ingeniería al Material rodante Férreo	• Se encarga de analizar y dar seguimiento a los trabajos de ingeniería de los trenes FM-95A	Algunas se han implementando recientemente para obtener y complementar mayores beneficios al mantenimiento y atención a usuarios.
• Centro de Información a Talleres	• Mantener una buena atención en todas las incidencias presentadas en el Departamento las 24 hrs. del día los 365 días del año.	
• Mantenimiento Mayor	• Estudio y análisis para el segundo Mantenimiento Mayor de Linea A de los trenes FM – 86.	
Macroproyectos del negocio		
• Tiempo Extra • Averías • Asistencia	• Captura, cálculo, reportes en sus diferentes modalidades para tener un control preciso de los gastos generados en el Departamento y para nomina de trabajadores. • Captura, Análisis y reportes de averías presentadas por tren, tipo de averías, frecuencia y clasificación de medidas tomadas así como en tiempo y forma • Reporte de incidencias, catorcenas del personal del departamento para su registro y control de asistencia.	Estos programas se han creado para facilitar el trabajo y agilización de los mismos. Cabe mencionar que no existe un área predeterminada como informático sino como apoyo, pero enfocada a labores tecnico administrativas y de apoyo informático por lo cual no se cuenta con los recursos necesarios suficientes para abarcar este aspecto y desarrollar mas programas.
Objetivos de la empresa		
• Brindar un buen servicio de transporte a usuarios • Mantener en buen estado y la imagen de los trenes por medio del mantenimiento preventivo y correctivo.	• Es un área propiamente de mantenimiento encargada de brindar un servicio de transporte masivo a usuarios.	

"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

Concepto	Descripción	Comentarios
Políticas referentes a la función de informática		
• Apoyar a las diferentes áreas de trabajo. • Compartir recursos e información. • Brindar servicio de atención a usuarios.	• Coadyuvar en el desarrollo informático y de apoyo en funciones y actividades de informática.	Debido a la plantilla incompleta del Departamento en general no existen políticas formalizadas en esta área.
áreas de oportunidad que se derivan de informática		
• Capacitar a los usuarios conforme sea necesario para el uso de la red. • Verificación periódica de todos los nodos y usuarios conforme programa de trabajo se establezca. • Mayor control de acceso para un mejor uso de la información. • Verificación del uso de Windows y paquetería acorde a las necesidades de cada área en específico • Listado de uso de cada uno de los equipos informáticos y responsables • Tener acceso a la información actualizada con las demás áreas de trabajo. • Disponibilidad de archivos generados por otros usuarios para agilizar el movimiento de la información. • Guardar archivos de importancia y además de interés para otras áreas en el servidor • Tener respaldos en el servidor sirve como protección contra algún posible daño que pudiera sufrir alguno de los equipos • Tener una impresora de red y que sirva para todos los equipos que no tiene en que realizar sus impresiones con calidad. • Acceso a la información las 24 hrs. del día los 365 días del año en algunos equipos con información relevante.	• Mantener buena comunicación e intercambio de información con las demás áreas de mantenimiento por medio de los apoyos informáticos con los que se cuenta y teniendo así información real con la debida actualización y en el momento preciso, así como el compartir hardware y software existente.	Se ha logrado beneficiar de gran manera al personal que labora directamente con los equipos informáticos teniendo al momento información actualizada para la toma de decisiones.

Este cuestionario tiene la finalidad de conocer ampliamente el estado en el que se encuentran los sistemas y equipos informáticos utilizados para las diferentes actividades de las áreas del taller, por lo cual se aplicó a las diferentes áreas del departamento, (ver los cuestionarios aplicados en el anexo 2).

A) Soluciones de Informática (Diagnóstico de los Talleres La Paz).

La finalidad de este cuestionario es tener un panorama mas amplio de cómo se encuentran distribuidos los recursos, personas y atención hacia los usuarios.

Instrucciones: Marque con una cruz en los recuadros la respuesta que crea usted más conveniente de acuerdo a su criterio.

	Calificación en base al grado de satisfacción			
Servicios	Excelente	Bueno	Regular	Deficiente
• Soluciones de consultoría Asesoría, apoyo técnico y soporte presentado por el apoyo informático en la evaluación y solución de problemas presentados	( )	( )	( )	( )
• Soluciones de sistematización y capacitación en procesos En la instalación de sistemas requeridos en el desarrollo de sus funciones operativas, tácticas y estratégicas	( )	( )	( )	( )
• Soluciones de desarrollo tecnológico Evaluación y selección de tecnología de vanguardia;	( )	( )	( )	( )
• Servicios operativos - Instalación de equipo de cómputo y telecomunicaciones - Capacitación en el uso de la tecnología - Atención a fallas de software y aplicaciones - Atención a fallas en equipos de cómputo y comunicaciones	( )	( )	( )	( )

B) Sistemas de información instalados "diagnóstico de informática"

INDICACIONES Contestar sólo por los conductores de los trenes.	SI	No
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	( )
Sistemas operativos de información Nombre (s) –Nivel Técnico.	( )	( )

C) Software instalado "Diagnóstico de información"

	Grado de satisfacción E,B,R,D	Número de máquinas con esta aplicación.	Usado por el D.S.M.M.R.F	usado por las coordinaciones	usado por el personal operativo
Procesador de palabras Nombre (s)			( )	( )	( )
Hojas de cálculo / graficadores Nombre (s)			( )	( )	( )
Lenguajes / manejadores de bases de datos Nombre (s)			( )	( )	( )
Presentador / textos Nombre (s)			( )	( )	( )
Correo electrónico / control de proyectos Nombre (s)			( )	( )	( )
Otros Nombre (s)					

D) Hardware instalado "Diagnóstico de información"

	Grado de Satisfacción E,B,R,D	Usado por el Depto	usado por las coordinaciones	usado por el personal operativo
Pc´s No. de estación de trabajo Cantidad Modelo(s)		( )	( )	( )
Procesador Cantidad Marca (s)		( )	( )	( )
Uso de Impresora Cantidad Modelo(s)		( )	( )	( )
Red (Si/No) ____ Tipo de Sistema Operativo: Windows NT ( ) Windows 95 ( ) Windows 98 ( ) Windows 3.11. ( )		( )	( )	( )

F) Capacitación / Actualización "Diagnóstico de información"

INDICACIONES Contestar sólo por los conductores de los trenes.	Excelente	Bueno	Regular	Deficiente
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	( )	( )	( )
Sistemas operativos de información Nombre (s) –Nivel Técnico.	( )	( )	( )	( )

G) Capacitación /Actualización "Diagnóstico de información"

INDICACIONES: Contestar de acuerdo a la capacitación recibida.

	Excelente	Bueno	Regular	Deficiente
Procesador de palabras Nombre (s)	( )	( )	( )	( )
Hojas de cálculo / graficadores Nombre (s)	( )	( )	( )	( )
Lenguajes / manejadores de bases de datos Nombre (s)	( )	( )	( )	( )
Presentador / textos Nombre (s)	( )	( )	( )	( )
Correo electrónico / control de proyectos Nombre (s)	( )	( )	( )	( )

Nombre: _____

Área: _____

CUADRO DE RESULTADOS DEL REPORTE DEL DIAGNÓSTICO PRELIMINAR DE LOS TALLERES LA PAZ DEL S.T.C.

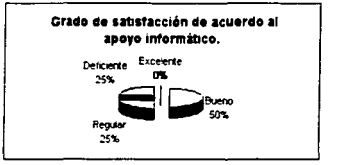
Criterios de Ponderación
E= Excelente B= Bueno R= Regular D= Deficiente

No	Sección	Pregunta	Número de personas que contestaron					
			E	B	R	D	SI	NO
1	A) Soluciones de Informática							
	Cómo califica usted los siguientes servicios prestados por el apoyo informático?	• Soluciones de consultoria	0	4	2	2		
		• Soluciones de sistematización y capacitación en procesos	0	3	4	1		
		• Soluciones de desarrollo tecnológico	0	1	3	4		
		• Servicios operativos.	0	3	2	3		
2	B) Sistemas de información instalados							
	¿Considera que los datos manejados en los programas y aplicaciones se procesan en un ambiente confiable , independientemente si son tacticos u operativos?	Sistemas tácticos de información.	0	1	0	0		
		Sistemas operativos de información.	0	1	0	0		
3	C) Software Instalado.							
	¿Cómo considera el rendimiento del software instalado en su máquina?	• Procesador de palabras	0	5	3	0		
		• Hojas de cálculo.	0	8	0	0		
		• Lenguajes manejadores de BD.	0	4	0	4		
		• Presentador de textos	0	7	1	0		
		• Correo Electrónico	0	2	0	6		
4	D) Hardware Instalado							
	¿Cómo considera el rendimiento del hardware que utiliza?	• Pc's	0	5	1	2		
		• Portatiles	0	1	0	0		
		• Procesador	0	5	3	0		
		• Impresora	0	7	1	0		
		• Sistema Operativo de Red	0	6	2	0		
5	E) Capacitación/actualización							
	¿Cómo califica la capacitación recibida en éstos paquetes?	• Procesador de palabras	0	1	3	4		
		• Hojas de cálculo.	0	2	2	4		
		• Lenguajes manejadores de BD.	0	1	2	5		
		• Presentador de textos	0	2	6	0		
		• Correo Electrónico	0	1	7	0		

A) SOLUCIONES DE INFORMÁTICA (DIAGNÓSTICO DE LOS TALLERES LA PAZ)

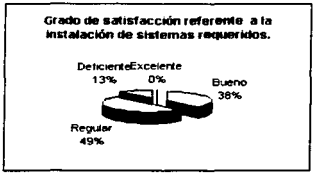
1.-Soluciones de consultoría.

Excelente	0
Bueno	4
Regular	2
Deficiente	2



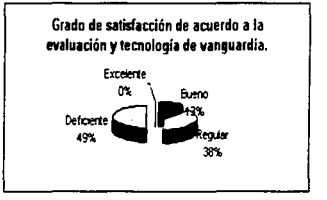
2.-Soluciones de sistematización y capacitación en procesos.

Excelente	0
Bueno	3
Regular	4
Deficiente	1



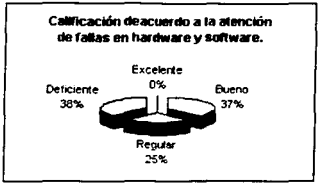
3.- Soluciones de desarrollo Tecnológico.

Excelente	0
Bueno	1
Regular	3
Deficiente	4



4.-Servicos Operativos.

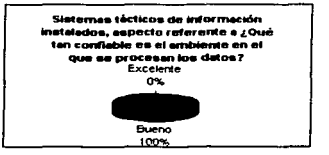
Excelente	0
Bueno	3
Regular	2
Deficiente	3



B) SISTEMAS DE INFORMACION INSTALADOS.

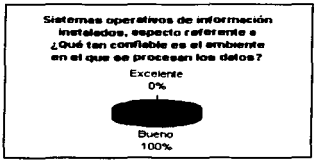
1.1 Sistemas tácticos de información.

Excelente	0
Bueno	1
Regular	0
Deficiente	0



1.2 Sistemas operativos de información

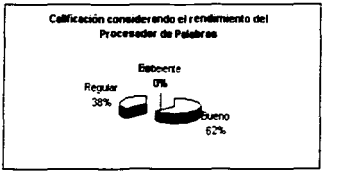
Excelente	0
Bueno	1
Regular	0
Deficiente	0



C) SOFTWARE INSTALADO.

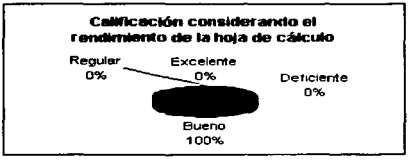
Procesador de Palabras

Excelente		0
Bueno		5
Regular		3
Deficiente	0	0



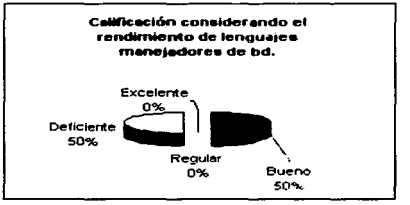
Hoja de cálculo

Excelente	0
Bueno	8
Regular	0
Deficiente	0



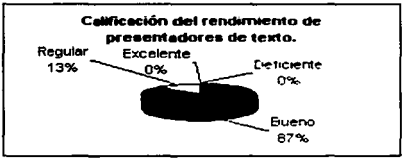
Lenguajes/manejadores de datos

Excelente	0
Bueno	4
Regular	0
Deficiente	4



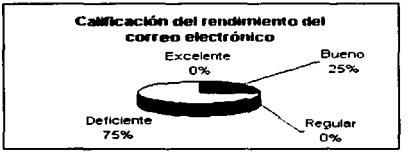
Presentadores de texto.

Excelente	0
Bueno	7
Regular	1
Deficiente	0



Correo electrónico

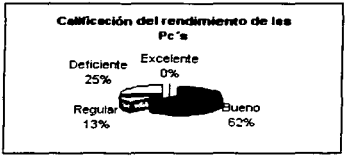
Excelente	0
Bueno	2
Regular	0
Deficiente	6



D) HARDWARE INSTALADO

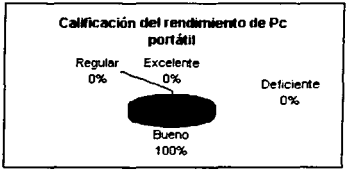
Pc´s

Excelente	0
Bueno	5
Regular	1
Deficiente	2



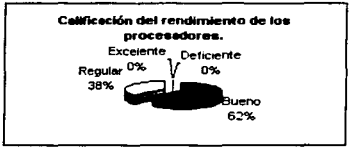
Pórtatiles

Excelente	0
Bueno	1
Regular	0
Deficiente	0



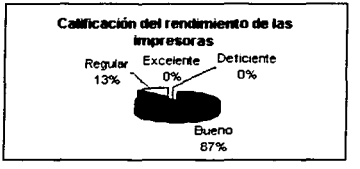
Procesador

Excelente	0
Bueno	5
Regular	3
Deficiente	0



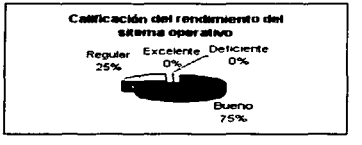
Impresora

Excelente	0
Bueno	7
Regular	1
Deficiente	0



Sistema operativo de red

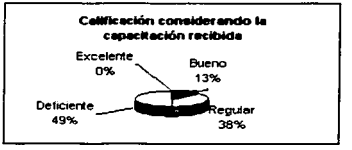
Excelente	0
Bueno	6
Regular	2
Deficiente	0



E) CAPACITACIÓN/ACTUALIZACION.

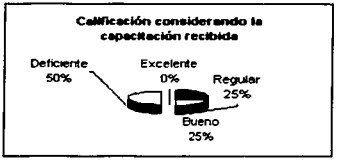
Procesador de palabras

Excelente	0
Bueno	1
Regular	3
Deficiente	4



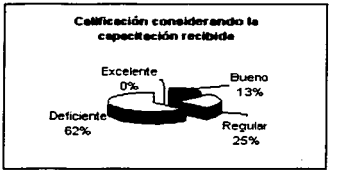
Hoja de cálculo

Excelente	0
Bueno	2
Regular	2
Deficiente	4



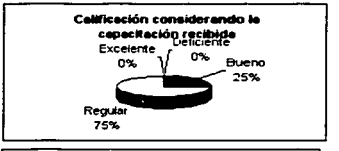
Lenguajes/manejadores de datos

Excelente	0
Bueno	1
Regular	2
Deficiente	5



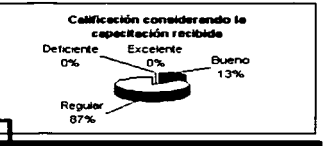
Presentadores de texto.

Excelente	0
Bueno	2
Regular	6
Deficiente	0



Correo electrónico

Excelente	0
Bueno	1
Regular	7



ANÁLISIS DEL REPORTE DE RESULTADOS DEL DIAGNÓSTICO PRELIMINAR (anexo 2)

Al realizar este análisis nos fue posible darnos cuenta de las áreas de oportunidad detectadas mediante las entrevistas practicadas así como a los usuarios que son clave dentro del departamento en esta primera etapa de la seguridad en informática, son (información recabada de los cuestionarios aplicados):

- Capacitar a los usuarios conforme sea necesario para el uso de la red.
- Verificación periódica de todos los nodos y usuarios conforme al programa de trabajo que se establezca.
- Mayor control de acceso para un mejor uso de la información.
- Verificación del uso de Windows y paquetería acorde a las necesidades de cada área en especifico.
- Listado de uso de cada uno de los equipos informáticos y responsables .
- Tener acceso a la información actualizada con las demás áreas de trabajo.
- Disponibilidad de archivos generados por otros usuarios para agilizar el movimiento de la información.
- Guardar archivos de importancia y además de interés para otras áreas en el servidor
- Tener una impresora de red y que sirva para todos los equipos que no tienen en que realizar sus impresiones con calidad.

Los sistemas de información instalados con los que se cuenta en Los Talleres son: Tiempo extra como sistema táctico, el cual se realizan actividades de captura, cálculo y reportes en diferentes modalidades para tener un control preciso de los gastos generados en el departamento y para nómina de trabajadores.

También se cuenta con un sistema de información operativo de averías en el que se maneja la captura, análisis y reportes de fallas presentadas, el tren en el que ocurrieron en tiempo e incidencia ocurrida.

Software instalado; en el DSMRF se encuentra instalado en Microsoft Office 97

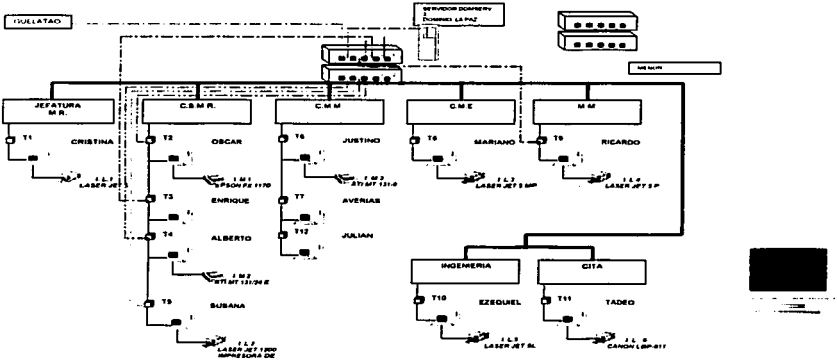
El hardware instalado en las diferentes áreas del DSMRF se compone de 14 computadoras personales y el servidor de red.

- De las cuales 8 cuentan con procesador Pentium ubicadas en la jefatura, CSMR, Mantenimiento menor, Electromecánica y el CITA.
- 3 que cuentan con procesador Ciryx 586 concentradas en CSMR y mantenimiento menor.
- 1 procesador 486Dx en CSMR.
- 1 procesador X86 Family 5 Model en CSMR.
- 1 Procesador Pentium 4 en CSMR.

El DSMMRF cuenta con una red de área local (LAN), la cual facilita la transmisión de datos, así como compartir recursos, archivos y programas. Utilizan la topología estrella donde todas las estaciones de trabajo se encuentran conectadas al concentrador con capacidad de 8 puertos, se compone de 12 nodos conectados independientemente de otras estaciones de trabajo y el cableado empleado en la red es el UTP o par trenzado y los conectores son RJ45.

Así mismo se cuenta con 9 impresoras para todo el Departamento de Servicios al Material Rodante entre las que destaca el tipo Lasser Jet en modelos (5, 1200, 5P, 5L ,5MP), Epson FX, ATI MT (2024751, 2004605) y Canon LBP-8II, las cuales se encuentran distribuidas como a continuación se ilustran.

REPRESENTACIÓN FÍSICA DE LOS EQUIPOS QUE CONFORMAN LA RED



PLAN DETALLADO (Detallar tareas y Tiempos)

En este estudio se ha contemplado una estructura de trabajo integral que permita a los usuarios tener la capacidad de resolver y desarrollar cualquier actividad de forma ágil y eficiente, considerando aquellos programas (software institucional oficial autorizado) de uso más generalizado que permita implementar una estructura estándar y sencilla para el uso de sus aplicaciones dentro de un ambiente operativo fácil, homogéneo e integrado que permita compartir información entre si, para evitar la dependencia hacia el personal calificado o responsable de la actividad de tal manera que todo el personal de los Talleres La Paz, cuente con los elementos necesarios para desarrollar sus actividades usando las computadoras como herramienta de trabajo y de mayor productividad.

A continuación se muestra esquemáticamente un diagrama de gantt acerca de los tiempos considerados para desarrollo del presente proyecto abarcando cada una de las etapas de seguridad que se consideran importantes abarcar

PLAN DETALLADO DE ACTIVIDADES

CALENDARIO DE ACTIVIDADES A REALIZAR DURANTE LA EJECUCIÓN DEL PROYECTO

ACTIVIDADES PRINCIPALES	PROG / REAL	TIEMPO APROXIMADO ESTIMADO: 7 MESES *(DEL 1 DEMARZO AL 30 DE SEPTIEMBRE DEL 2002)*																											
		MAR				ABR				MAY				JUN				JUL				AGO				SEP			
SEMANAS		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
SEGURIDAD FÍSICA DE LAS INSTALACIONES Y EQUIPOS	P																												
	R																												
ACTIVIDADES SECUNDARIAS: Distribución de equipo informático, centros de proceso, servidor, terminales																													
ACTIVIDADES SECUNDARIAS: Control de personal interno y externo																													
ACTIVIDADES SECUNDARIAS: Verificación de Equipos de seguridad																													
ACTIVIDADES SECUNDARIAS: Fallas en energía eléctrica																													
ACTIVIDADES SECUNDARIAS: Control del Software institucional y Aplicaciones																													
ACTIVIDADES SECUNDARIAS: Control de personal de entrada y salida																													
ACTIVIDADES SECUNDARIAS: Protección de soportes magnéticos y documentación																													
ADMINISTRACIÓN DE CAMBIOS Y PROBLEMAS	P																												
	R																												
ACTIVIDADES SECUNDARIAS: Organización de personal																													
ACTIVIDADES SECUNDARIAS: Administración de usuarios																													
ACTIVIDADES SECUNDARIAS: Acceso público																													
CONTROLES DE SEGURIDAD DE ACCESO LÓGICO	P																												
	R																												
ACTIVIDADES SECUNDARIAS: Respaldo de información																													
ACTIVIDADES SECUNDARIAS: Control y asignación de contraseña																													
ACTIVIDADES SECUNDARIAS: * Longitud																													
ACTIVIDADES SECUNDARIAS: * Frecuencia de cambio																													
ACTIVIDADES SECUNDARIAS: * No. De intentos permitidos al usuario																													
ACTIVIDADES SECUNDARIAS: Control de acceso a los usuarios (Equipos Físicos) Hardware y software																													
ACTIVIDADES SECUNDARIAS: Detección de virus																													
ACTIVIDADES SECUNDARIAS: Control de permiso hacia la información																													
ACTIVIDADES SECUNDARIAS: Estandarización de nombres de los equipos de acuerdo al área																													

PLAN DETALLADO DE ACTIVIDADES

CALENDARIO DE ACTIVIDADES A REALIZAR DURANTE LA EJECUCIÓN DEL PROYECTO

	ACTIVIDADES PRINCIPALES	PROG / REAL	TIEMPO APROXIMADO ESTIMADO: 7 MESES *(DEL 1 DE MARZO AL 30 DE SEPTIEMBRE DEL 2003)*																									
			MAR				ABR				MAY				JUN				JUL				AGO				SEP			
		SEMANAS	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
	SEGURIDAD EN DATOS (CLIENTE/SERVIDOR)	P																												
		R																												
ACTIVIDADES SECUNDARIAS	Donde y como se genera la información																													
ACTIVIDADES SECUNDARIAS	Control de documentación impresa																													
ACTIVIDADES SECUNDARIAS	Clasificación de información																													
ACTIVIDADES SECUNDARIAS	Origen, proceso y salida de los datos, destino																													
	SEGURIDAD EN COMUNICACIONES	P																												
		R																												
ACTIVIDADES SECUNDARIAS	Enlaces, concentradores, conmutadores y servidores																													
ACTIVIDADES SECUNDARIAS	Restricción de dominios con accesos correspondientes																													
ACTIVIDADES SECUNDARIAS	Software pirata																													
ACTIVIDADES SECUNDARIAS	Información ajena a las fnciones de su competencia de acuerdo al personal y actividades asignadas																													
ACTIVIDADES SECUNDARIAS	Información ajena a las funciones de su competencia																													
ACTIVIDADES SECUNDARIAS	Tipo de red																													
ACTIVIDADES SECUNDARIAS	Conexiones																													
ACTIVIDADES SECUNDARIAS	Ambiente Sistema Operativo																													
ACTIVIDADES SECUNDARIAS	Transferencia de archivos																													
ACTIVIDADES SECUNDARIAS	Control de información publica																													
	PLANES DE SEGURIDAD EN CONTINUIDAD DE LAS OPERACIONES	P																												
		R																												
ACTIVIDADES SECUNDARIAS	Tipo de respaldo de información																													
ACTIVIDADES SECUNDARIAS	Existencia de algun plan de contingencia por área o Taller																													
ACTIVIDADES SECUNDARIAS	Contar con recursos humanos y materiales																													
ACTIVIDADES SECUNDARIAS	Catalogo de incidencias																													
	ADMINISTRACION DE LA SEGURIDAD	P																												
		R																												
ACTIVIDADES SECUNDARIAS	Base de datos																													
ACTIVIDADES SECUNDARIAS	Redes de procesamiento																													
ACTIVIDADES SECUNDARIAS	Internet																													
ACTIVIDADES SECUNDARIAS	Personal-Equipamiento																													
	SEGURIDAD EN INTERNET	P																												
		R																												
ACTIVIDADES SECUNDARIAS	Autorización																													
ACTIVIDADES SECUNDARIAS	Integridad de datos																													
ACTIVIDADES SECUNDARIAS	Privacidad de datos																													

ÁREAS DE LOS TALLERES "LA PAZ"

BENEFICIADAS DIRECTAMENTE CON LA IMPLEMENTACIÓN DE ESTE PROYECTO:

COORDINACIÓN DE SERVICIOS AL MATERIAL RODANTE
COORDINACIÓN DE MANTENIMIENTO MENOR
COORDINACIÓN DE MANTENIMIENTO ELECTROMECÁNICO
COORDINACIÓN DE INGENIERÍA Y ASEGURAMIENTO DE LA CALIDAD
CENTRO DE INFORMACIÓN A TALLERES (C.I.T.A.)

REALIZO

Susana Flores Leal

Vo. Bo.

Ing. Gerardo J. Chacon Cruz

TÉCNICAS Y HERRAMIENTAS UTILIZADAS

Se realizaron por medio de:

Entrevistas.- Las cuales se realizaron directamente con cada uno de los usuarios para determinar cuales eran las dificultades que se presentaban normalmente y atendiendo en el momento las que tenían solución.

Cuestionarios.-Esto se realiza por medio de lograr un acercamiento con los usuarios a fin de lograr determinar una situación global y teniendo los antecedentes (evidencias) de la problemática que se expone.

Encuestas.- Por medio de los cuestionarios creados para tal fin en cada una de los tipos de seguridad a analizar.

Investigación de campo.- En cada uno de los equipos y con los usuarios de los mismos.

Documentación: como apoyo para complementar el trabajo con avances previos en caso de existir en algún caso en particular, Programas de trabajo de las distintas áreas, organigramas, manuales, minutas de proyectos anteriores.

Visor sucesos.- Este toma como auxiliar para determinar lo que ocurre en el entorno de red.

DEFINICIÓN Y DETERMINACIÓN DEL TAMAÑO DE LA MUESTRA A ANALIZAR.

Se define que la población actual que utiliza los equipos de cómputo para realizar sus actividades en los talleres La Paz del (Sistema de Transporte Colectivo METRO) es de 25 personas distribuidas en las 6 diferentes coordinaciones.

Para éste proyecto se utilizó una muestra probabilística debido a que tiene la ventaja de que se puede medir el tamaño del error de las predicciones que se hagan. El principal objetivo de este tipo de muestreo es el de reducir al mínimo este error denominado también error estándar

A continuación se explican las fórmulas que fueron necesarias para determinar el número aproximado de personas que se creyó conveniente entrevistar, donde:

N	=	Población	n	=	Muestra
n^1	=	Muestra provisional	V^2	=	Varianza
Se	=	Error Standard	S^2	=	Varianza de la muestra
p	=	Probabilidad de ocurrencia			

Margen de error "se".	0.09	
Acercamiento a la población "p".		0.9
Tamaño de la población "N".	25	

Varianza de la muestra:	acerca .a la pob.	
S^2* p(1-p)	0.9	0.10
Varianza:	margen de e.	V^2
V^2* (se)^2	0.09	0.0081

Muestra provisional		
$n1= (s^2/v^2)$	12.3456790	
Muestra	tam. De pob	
$n= (n^1)/(1+[n^1/N])$	25	
Tamaño de la Muestra: =	**8.26446281**	

FORMATOS DE TRABAJO PARA SER APLICADOS Y ANALIZAR LA SEGURIDAD QUE EXISTE ACTUALMENTE

Como Información general hay 74 personas con categoría de base y 18 personas de confianza dando un total de 92 personas, pero únicamente 25 personas hacen uso del equipo informático los demás son de índole técnico operativo en las áreas de mantenimiento. (Ver cuestionarios aplicados en el Anexo 3)

"CUESTIONARIO DE SEGURIDAD FÍSICA"

Instrucciones: Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).

A) Ubicación y construcción de las instalaciones.

1. ¿El edificio cuenta con salidas de escape en caso de emergencia?
   Si ( ) No ( )
2. ¿Existen ventanas grandes que permitan la entrada del sol directamente en los equipos?
   Si ( ) No ( )

B) Aire acondicionado.

3. ¿Los dúctos de aire se encuentran libres de polvo?
   Si ( ) No ( )

C) Instalación eléctrica y suministro de energía.

4. ¿Se cuenta con tierra física?
   Si ( ) No ( )
5. ¿Los cables se encuentran debidamente identificados (positivo, negativo, tierra física)?
   Si ( ) No ( )
6. ¿Los contactos del equipo de cómputo están debidamente identificados?
   Si ( ) No ( )
7. ¿Se tiene conectado a los contactos de equipo de cómputo con otro equipo electrónico?
   Si ( ) No ( )
8. ¿Se tienen reguladores para los equipos de cómputo?
   Si ( ) No ( )
9. ¿Se tiene equipo No-break?
   Si ( ) No ( )
10. ¿Aproximadamente cuánto es el tiempo que se da para respaldar los archivos o para continuar el proceso?
    a) 15 minutos ( ) b) 30 minutos ( ) c) 1 hora ( )
11. ¿Los cables están dentro de los paneles y canales eléctricos?
    Si ( ) No ( )

D) Autorización de accesos.

12. ¿Existe personal de vigilancia en la institución?
    Si ( ) No ( )
13. ¿Se identifica a la persona que ingresa?
    Si ( ) No ( )

E) Extintores.

14. ¿Existen extintores de fuego?
    a) Manuales ( ) b) Automáticos ( ) c) No existen ( )
15. ¿Se ha capacitado al personal en el manejo de éstos?
    Si ( ) No ( )
16. ¿Los extintores funcionan a base de?
    a) Agua ( ) b) Gas ( ) Otros (menciónelos)_____
17.- ¿Se han tomado medidas para minimizar la posibilidad de fuego?
    a) Evitando artículo inflamables ( )
    b) Prohibiendo fumar en las áreas de riesgo ( )
    c) No se ha previsto ( )

"CUESTIONARIO DE ADMINISTRACIÓN DE CAMBIOS Y PROBLEMAS EN APLICACIONES"

Instrucciones: Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).

A) Controles y procedimientos utilizados.

1. Se cuenta con controles y procedimientos necesarios para garantizar la seguridad mínima requerida?

	Si	No
a) Procedimiento de llenado de documentos.	( )	( )
b) Procedimiento de encendido y apagado de la computadora.	( )	( )
c) Reinicialización del equipo en caso de fallas.	( )	( )

2. ¿Se cuentan con procedimientos para asegurar que los cambios en aplicaciones se documenten?

	Si	No
a) Se encuentran justificados por medio de requerimientos de los usuarios.	( )	( )
b) Se encuentran descritos mencionando el objetivo y función de éstos.	( )	( )
c) Se encuentran probados antes de ser implantados formalmente.	( )	( )
d) Se tienen en existencia manuales de referencia para el usuario.	( )	( )

B) Procesamiento de la información.

3. ¿Se asegura que sólo los responsables de modificar los programas tengan acceso a éstos, explique de que forma?

Si ( ) No ( )

4. ¿Quién se encarga de efectuar las siguientes modificaciones a programas y aplicaciones?

	Actualización	Eliminación	Consulta	Captura
Los mismos usuarios	( )	( )	( )	( )
El encargado (a) de brindar apoyo informático	( )	( )	( )	( )
Programadores	( )	( )	( )	( )
Otros	( )	( )	( )	( )

5. ¿Quién es el encargado de dar asistencia para la soluciones de problemas y aplicaciones que usted utiliza?
   a) La encargada de apoyo informático. ( )
   b) Usted mismo. ( )

6. ¿Cuál es el estado que alcanza el o los problemas suscitados en las aplicaciones que utiliza?
   a) Resuelto, usted está trabajando de nuevo, pero el problema aún sigue latente. ( )
   b) Cerrado se han realizado cambios para que ningún otro usuario tenga el mismo problema. ( )

C) Seguridad en archivos.

7. ¿Se cuenta con procedimientos de respaldo de programas fuente, documentación y archivos en operación, menciónelos?

Si ( ) No ( )

8. ¿Se encuentra en un lugar distante el almacenamiento de copias de los archivos?

Si ( ) No ( )

9. ¿Existen bitácoras para tener un control por escrito de las modificaciones hechas a programas y aplicaciones?

Si ( ) No ( )

"CUESTIONARIO DE SEGURIDAD LÓGICA".

Instrucciones: Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).

1. ¿Se controla el préstamo de:
   a) Elementos magnéticos ( )
   b) Equipo ( )
   c) Software ( )
2. ¿Se cuenta con copias de los archivos en un lugar distinto al de la computadora?
   Si ( ) No ( )
3. ¿Se tienen establecidos procedimientos de actualización para estas copias?
   Si ( ) No ( )
4. ¿Se elabora un análisis del perfil del usuario para tener acceso a la información?
   Si ( ) No ( )
5. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones?

	Si	No
a) Recepción de documentos	( )	( )
b) Información confidencial	( )	( )
c) Captación de documentos	( )	( )
d) Programas	( )	( )
e) Documentos de salida	( )	( )
f) Archivos magnéticos	( )	( )

6. ¿Existe un responsable de asignación de claves de acceso al equipo?
   Si ( ) No ( )
7. ¿Se lleva un control sobre las claves asignadas?
   Si ( ) No ( )
8. ¿Existe un cambio periódico en las claves de acceso?
   Si ( ) No ( )
9. Existen copias mensuales de archivos históricos de la información?
   Si ( ) No ( )
10. ¿Existen técnicas de encripción para datos?
    Si ( ) No ( )
11. ¿Existen registros con información relevante para el administrador de la red, si es así Quién los genera?
    Si ( ) No ( )
    a) Algún tipo de software ( )
    b) Por los responsables del sistema ( )
12. ¿Se protege el acceso a librerías del sistema?
    Si ( ) No ( )
13. ¿Se tiene un control para determinar las rutas de acceso al sistema?
    Si ( ) No ( )
14. ¿En lo que se refiere a sistemas de información se cuenta con un campo de validación para acceder a la información?
    Si ( ) No ( )
15. ¿Existen controles de acceso al diccionario de datos?
    Si ( ) No ( )
16. En cuanto al proceso de identificación del usuario:
    a) Se revocan usuarios inactivos ( )
    b) Se despliega la última fecha en que se tiene acceso. ( )

"CUESTIONARIO PARA VERIFICAR LA SEGURIDAD CLIENTE-SERVIDOR"

Instrucciones: Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).

1. ¿Cuantas estaciones de trabajo existen en la red? _____

2. ¿Con que tipo de servidor se cuenta?
   a) Dedicado ( )
   b) No dedicado ( )

3. ¿Se hace uso del servidor como cliente cuando realiza una solicitud de servicio a otras plataformas dentro de la red?
   Si ( ) No ( )

4. ¿Se ha escalado la infraestructura de la red?
   Si ( ) No ( )

¿Qué proyectos se tienen contemplados para el crecimiento de la infraestructura computacional?
_____

5. Se han presentado alguno de éstos problemas:
   a) Congestionamiento en la red. ( )
   b) Dificultad para el tráfico de los datos. ( )

6. ¿Ha habido migración de aplicaciones a otras plataformas?
   Si ( ) No ( )

7. ¿Existe algún tipo de control ya sea físico, lógico o administrativo para los datos usados en las PC para reforzar la seguridad de acceso.
   Si ( ) No ( )

8. ¿Existe un responsable encargado de mantener la integridad de los datos y aplicaciones distribuidas en red?
   Si ( ) No ( )

9. ¿Se establecen políticas y procedimientos de seguridad en el servidor, así como en las estaciones de trabajo?
   Si ( ) No ( )

10. ¿El sistema de red LAN soporta las aplicaciones de alto procesamiento transaccional?
    Si ( ) No ( )

11. ¿Qué servicios de datos e impresión comparte?
    a) Archivos ( )
    b) Base de datos ( )
    c) Impresoras ( )
    d) Plotters ( )
    e) Administración de colas de impresión en diferentes dispositivos ( )

12. ¿Qué tipo de protocolo utiliza la red?_____

13. ¿Se permite la transportación de aplicaciones de un procesador a otro, sin que éste se modifique?
    Si ( ) No ( )

"CUESTIONARIO DE SEGURIDAD EN LA RED".

Instrucciones: Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).

1. ¿Hay procedimientos que protejan los datos transmitidos en la red, si es así menciónelos?
   Si ( ) No ( )
2. ¿Existen registros con información relevante sobre el comportamiento de la red?
   Si ( ) No ( )
3. ¿La red tiene controles de acceso a datos no autorizados?
   Si ( ) No ( )
4. ¿Existen controles relativos a la seguridad física de los diversos componentes de la red como lo son tarjetas, terminales, manuales, teclados, ratones, etc?
   Si ( ) No ( )
5. ¿Se tiene un seguro que proteja el software y equipo de red?
   Si ( ) No ( )
6. ¿Se cuenta con alternativas que apoyen al Departamento en caso de alguna falla generalizada y prolongada en la red?
   Si ( ) No ( )
7. ¿Se verifica la identificación de terminales y usuarios?
   Si ( ) No ( )
8. ¿Se registra la violación de procedimientos de acceso a las máquinas con el fin de llevar una estadística y frenar tendencias?
   Si ( ) No ( )
9. ¿Se cuenta con manuales de operación de la red?
   Si ( ) No ( )
10. ¿Fue capacitado y preparado el personal para administrar y operar la red?
    Si ( ) No ( )
11. ¿Se evalúa el desempeño de la red en medida del tiempo de respuesta y recuperación de la misma?
    Si ( ) No ( )
12. ¿Se da un mantenimiento a la red, donde se indiquen las fechas y responsables para hacerlo?
    Si ( ) No ( )
13. ¿Se han tomado en cuenta algunas consideraciones complementarias que ayuden al mejoramiento continuo de la red local como las siguientes?

	Si	No
a) Evaluación periódica de la red: hardware, software, grado de utilización.	( )	( )
b) Acceso de nuevos usuarios a la red, niveles de perfil de usuario, asignación de software o datos para utilizar, consultar, borrar, modificar.	( )	( )
c) Capacitación, planeación, ejecución y actualización.	( )	( )
d) Crecimiento de la red: periféricos, memoria, usuarios, aplicaciones	( )	( )
e) Respaldo: datos, equipo, periféricos, software, aplicaciones.	( )	( )
f) Seguridad en el procesamiento, planes de recuperación.	( )	( )

14. Señale si tiene identificada formalmente la siguiente información:

	Si	No
a) Usuarios de la red	( )	( )
b) Registro y niveles de acceso.	( )	( )
c) Terminales conectadas a la red	( )	( )
d) Responsables de la red	( )	( )
e) Procedimientos de contingencia	( )	( )
f) Software	( )	( )
g) Periféricos conectados	( )	( )
h) Software original y pirata instalado	( )	( )
i)Tipos de unidades centrales de procesamiento	( )	( )
j) Capacidad de disco o espacio libre en el servidor	( )	( )

"CUESTIONARIO DE ADMINISTRACIÓN DE LA SEGURIDAD"

Instrucciones: Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).

1. ¿Existe una función de investigación dedicada a la evaluación de software, métodos y procedimientos sugeridos en el mercado para la implantación de acciones relativas a la seguridad que brinden un cuidado a los recursos relacionados con la informática?
   Si ( ) No ( )
2. ¿Existe administración formal de la red?
   Si ( ) No ( )
3. ¿En caso de no tener una administración formal de la red, ¿Se da el seguimiento a los siguientes aspectos?

	Si	No
a) Planeación de nueva tecnología de la información (hardware y software)	( )	( )
b) Monitoreo de las actividades de la operación y mantenimiento de la red	( )	( )
c) Procedimientos y control de seguridad	( )	( )
d) Aspectos legales del software instalado	( )	( )
e) Capacitación y soporte a usuarios	( )	( )

4. ¿Existe alguna persona externa que intervenga en la administración de la red?
   Si ( ) No ( )
5. ¿Existe la documentación formal que especifique qué hacer y cómo efectuar las funciones administrativas de la red?
   Si ( ) No ( )
6. ¿Se elaboran políticas y procedimientos de seguridad referente a datos, aplicaciones, hardware, software y accesorios de la red?
   Si ( ) No ( )
7. ¿Cómo se canalizan las dudas, sugerencias y compromisos entre usuarios y responsables de la red? _____
   _____
8. ¿Existe una persona encargada de administrar la red?
   Si ( ) No ( )
9. ¿Se tiene un control en cuanto al número de horas en las que los usuarios inicien sesiones en la red?
   Si ( ) No ( )
10. ¿Existen estrategias de organización para usuarios o grupos de usuarios?
    Si ( ) No ( )
11. ¿Se tiene implementado algún plan de cuentas para proteger la red?
    Si ( ) No ( )
12. ¿En el caso de contar con carpetas compartidas existe una jerarquía en estas?
    Si ( ) No ( )
13. ¿Se controla el acceso a aplicaciones y datos?
    Si ( ) No ( )
14. ¿Se han organizado los recursos de disco a fin de que las carpetas que tengan los mismos requisitos de seguridad se ubiquen dentro de una misma jerarquía?
    Si ( ) No ( )
15. ¿Se ha documentado que usuarios y permisos se tienen para acceder recursos?
    Si ( ) No ( )
16. ¿Se han establecido directivas de seguridad para asignar permisos de impresión?
    Si ( ) No ( )
17. ¿Se han contemplado planes de seguridad para archivos, directorios, impresoras y controladores de dominio?
    Si ( ) No ( )

"CUESTIONARIO DE SEGURIDAD EN INTERNET".

Instrucciones: Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).

1.- ¿Cuenta su equipo con un antivirus actualizado?
Si ( ) No ( )

2.- ¿Qué tipo de navegador de red utiliza?

Netscape ( )
Explorer ( )
MSN Explorer ( )
Otro ( ) Menciónelo _____

3.- ¿Se utilizan programas de seguridad para controlar las Cookies que envían datos devuelta a los sitios Web?
Si ( ) No ( )

4.- ¿Se garantiza la transferencia segura de información al usuario final?
Si ( ) No ( )

5.- ¿Se cerciora de obtener información relativa del nivel de seguridad existente en el servidor que hospeda las páginas que usted?
Si ( ) No ( )

6.- ¿Al intercambiar información verifica lo siguiente?

		Si	No
a)	El cambio de protocolo HTTP en la ventana de direcciones	( )	( )
b)	Que exista un icono de seguridad (candado o llave de navegador)	( )	( )

7.- ¿Se ha fomentado el uso de certificados personales de seguridad para proteger su identidad en Internet?
Si ( ) No ( )

8.- ¿Qué es lo que realiza generalmente cuando descarga un archivo?
a) Lo abre desde el origen ( )
b) Lo guarda en disco ( )

9.- ¿Con qué dispositivos de seguridad se cuenta?
a) Repetidores ( )
b) Concentradores (hub's) ( )
c) Puentes (Bridges) ( )
d) Encaminadotes (routers) ( )
e) Pasarela Gateway) ( )

"CUESTIONARIO PARA VERIFICAR LOS PLANES DE CONTINUIDAD DEL NEGOCIO".

Instrucciones: Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).

A) Operaciones fundamentales.

1. ¿Cuál es el impacto de una hora de interrupción en los equipos de su área de trabajo?
   a) Tener al personal totalmente parado ( )
   b) Es inconveniente, pero las actividades en el departamento continúan ( )
   c) No altera en lo absoluto ( )

2. ¿Cuál es el impacto de la interrupción total en los equipos de cómputo, durante varias semanas?
   a) Critica, no hay fuentes de respaldo ( )
   b) Existen facilidades de respaldo externas, pero origina mayores costos ( )

3. ¿Cuál es la aptitud del personal ante una situación de emergencia?
   a) Se organizan ( )
   b) Se organizan a medias ( )
   c) Son desorganizados ( )
   d)

4. La localización de sistemas se encuentra en:
   a) Un área especifica ( )
   b) En dos o más áreas ( )
   c) Se encuentran en todo el departamento ( )

5. ¿Cuál es el tiempo que tarda en reanudarse después de una interrupción, de cortes de energía eléctrica o caída del sistema?
   a) 3 o 4 días vuelve a la normalidad ( )
   b) En 12 o 24 días ( )
   c) La recuperación es casi inmediata ( )

¿Cómo es el control después

6. de una interrupcion?
   a) El daño es controlado de forma rápida ( )
   b) Es muy difícil de recuperar ( )
   c) Es posible mediante copias manuales ( )

CONCLUSIONES CAPÍTULO III

En este capítulo se aplicó un cuestionario de diagnóstico actual para saber de manera específica las áreas que comprenden el taller, los programas y aplicaciones en uso y la forma en que se utilizaban, los cuales se aplicaron a los responsables de los equipos informáticos, dando como resultado puntos clave que determinan el uso de los recursos y la información en general, a la que se llego fue la falta de: capacitación al personal, actualización de equipos, personal que se encargue de dar mantenimiento a los equipos y a algunos recursos físicos como impresoras, scanner, plotter, unidades de respaldo entre otros, etc.

De igual forma, se aplicaron 8 tipos de cuestionarios de cada rubro de seguridad a ser evaluados, los cuales fueron de opción múltiple para facilitar sus respuestas y ahorro de tiempo que ayudaron en gran medida para tener una visión amplia, en lo que se refiere a Seguridad Física, Administración de cambios y Problemas en aplicaciones, Seguridad Lógica, Seguridad Cliente-Servidor, Seguridad en Red, Administración de la Seguridad, Seguridad en Internet y planes de continuidad en el negocio; de los cuales ha sido posible percatarse que la seguridad en cada una de las etapas es poca, por lo cual realmente existen riesgos latentes y que es necesario ponerles atención a fin de lograr en un momento determinado, reducir las debilidades y convertirlas en fortalezas, esto sólo es posible lograrlo con la colaboración de todos, además de los conocimientos suficientes para guiarlos en cada proceso, poniendo mayor atención en los que representan mayor peligro.

La evaluación de resultados es muy importante, ya que implica necesariamente la existencia de parámetros de referencia contra los cuales comparar y juzgar lo obtenido para ver que tan efectivos han resultado los procesos de trabajo llevados a cabo hasta el momento, o bien para realizar los ajustes y probar la estrategia elegida y además comprobar que tan efectiva será y de esta manera tener los elementos disponibles para tomar decisiones acertadas

En el siguiente capítulo se plantean algunas de las ventajas que van acorde al desarrollo e implantación, se mencionaran los aspectos o componentes a ser evaluados, así como la realización de un informe a fin de lograr la Seguridad Informática y algunas recomendaciones generales.

CAPITULO IV

DESARROLLO E IMPLEMENTACION

CAPÍTULO IV.- ETAPA DE DESARROLLO E IMPLEMENTACIÓN

Aquí se ejecutan las tareas de trabajo de acuerdo con el plan aprobado en la etapa de formalización. Además de la importancia que tiene para los involucrados, ya que los responsables de las áreas usuarias y de informática ahora serán los encargados de ejecutar las acciones recomendadas en los informes presentados y aprobados a la alta dirección, así como diferenciar y clasificar acciones inmediatas a corto y mediano plazo.

- Concertación de fechas de entrevistas, visitas y aplicación de cuestionarios.
- Verificación de las tareas.
- Clasificación de técnicas, cuestionarios, entrevistas.
- Elaboración de un informe.
- Revisión de dicho informe.
- Clasificación y documentación del informe.
- Finalización de tareas.
- Elaboración de un informe final.
- Presentación del informe a participantes y a la alta dirección.
- Aprobación final del proyecto general.

ACCIONES

- Basarse en el plan de seguridad elaborada anteriormente (en caso de existir).
- No interrumpir la continuidad de las operaciones de la empresa.
- Apoyo al trabajo con políticas y estándares comúnmente aceptados.
- Involucrar a usuarios y personal de informática según lo amerite la tarea a ejecutar.
- Las entrevistas son de manera profesional y adecuada al perfil de cada entrevistado.
- Al visitar áreas de trabajo se respetan las políticas que imperan en ese medio.
- Analizar con objetividad los escenarios emanados de la aplicación de cuestionarios, entrevistas y visitas realizadas.

CONTENIDO DE LOS INFORMES

- áreas de oportunidad para mejora inmediata.
- Observaciones (debilidades y carencias) de los aspectos de informática
- Recomendaciones preliminares.
- Involucrados, así como una comunicación abierta con ellos.
- Causas que están originando las debilidades y carencias, su problemática.

PUNTOS DE INFORMÁTICA A EVALUAR

- Sistemas de Información.
- Operación o mantenimiento.
- Seguridad.
- Planes de contingencia y recuperación en caso de desastres.
- Administración de la función informática.
- Planeación Informática.
- Organización Informática.

ETAPAS PARTICULARES A CONSIDERAR DURANTE LA FASE DE DESARROLLO:

- Comunicaciones
- Redes locales
- Investigación de Tecnología
- Usuarios de Informática.

Todo este análisis se desarrolla, considerando lo que ya existe en las instalaciones de los Talleres la Paz del Sistema de Transporte Colectivo Metro.

La mejor y más eficaz forma de alcanzar el mayor provecho de los recursos y además mantenerlo, es usando las herramientas mas actuales de seguridad informática y actualización tecnológica a fin de estar siempre a la vanguardia para poder implementar este proyecto directamente en toda la red actual, de tal forma que los procedimientos de trabajo sean cada vez más versátiles, sencillos y eficientes.

VENTAJAS

A continuación se mencionan algunas de las ventajas que se encontraron

- Se cumplirán los requerimientos establecidos.
- Se aprovecharan los recursos humanos con que cuenta la empresa.
- El mantenimiento será inmediato y no se ocasionaran costos extras.
- No se generará dependencia externa.
- Se realizará con la ventaja de contar con los conocimientos y experiencia previos de la seguridad para llevar a buen fin su funcionalidad e implantación.
- Podrá ser implantado en un tiempo relativamente corto pensando en el tiempo que se a trabajado sin control.
- Se adaptará perfectamente a las necesidades de las instalaciones.
- Los errores que puedan surgir se corregirán a tal grado, que exista lo más mínimo en cuestión de fallas.
- El costo que todo este desarrollo implicara, será más económico que si se contratará asesoría externa para desarrollarlo e implantarlo, considerando que alguien externo tendría que estudiar a fondo la estructura, organización y características, de la red instalada y su seguridad
- La seguridad en informática se apegará completamente a cubrir y resolver la problemática existente.
- Se podrán identificar nuevos requerimientos, con lo cual se mejorará el desempeño de las terminales.

OBJETIVOS

- La seguridad en informática determinará los problemas existentes.
- Con el análisis y desarrollo se pretende lograr que la red de cómputo (LAN) funcione de manera óptima, con los recursos de hardware y software actualmente disponibles.
- Al realizar la estructuración se logrará permitir la amplia posibilidad de mantenimiento de la red.

INFORME DE ACTIVIDADES FIN DE LOGRAR LA SEGURIDAD INFORMÁTICA

Con el desarrollo e implementación se pretende lograr compartir datos de todos los sistemas principales de cada coordinación, esto con la finalidad de contar con información actualizada y confiable, es decir; cada coordinación es responsable de la certeza e integridad de la información que maneja, de manera reciproca recibirá datos actualizados para compartir, así como la información que se genere en otras coordinaciones, los beneficios de esta implantación son los siguientes:

- Evitar la realización innecesaria de información ya existente.
- Evitar duplicidad de funciones y trabajo (generando trabajo extra).
- Contar con la información actualizada y confiable desde su origen.
- Generar tiempo para el procesamiento de la información.
- Reducir tiempos de espera
- Simplificación de gastos en recursos materiales e informáticos

INVENTARIO DE RIESGOS

Se realizo un análisis del estado actual de la Seguridad Informática existente en el Departamento de Servicios de Mantenimiento al Material Rodante obteniendo lo siguiente:

No	CIRCUNSTANCIAS	RIESOS
01	Virus informático en red y equipos locales	• Daño de archivos • Pérdida de información.
02	Falta de actualización de respaldos y en algunos casos inexistencia de éstos.	• Atraso en la información para cumplir con trabajos, en tiempo y forma.
03	Software pirata	• Problemas legales. • Falta de documentación.
04	1. Falta de control en acceso físico de personal a área de cómputo. 2. Conocimiento de password por todos los usuarios.	• Mal uso de la información. • Borrado y copiado de información confidencial.
05	No existe segregación de funciones (dependencia hacia algunos usuarios)	• Dependencia hacia personal que maneja proyectos clave.
06	Inexistencia de planes de contingencia en caso de desastre.	• Pérdida de tiempo para reiniciar actividades.
07	Falta de políticas de seguridad	• Seguimiento nulo o informal de proyectos.
08	1. Comer en el área de cómputo y polvo en equipos. 2. Manipulación errónea de equipo por desconocimiento de uso apropiado.	• Deterioro y pérdida de equipos o componentes.
09	Inexistencia de catalogo de jerarquías en red.	• Acceso a recursos y programas no permitidos.
10	1. Depuracion de archivos temporales. 2. Obsolescencia de hardware y software.	• Lentitud en el procesamiento de trabajo

RECOMENDACIONES Y ACCIONES TERMINADAS
(PLAN DE SEGURIDAD INFORMÁTICA A SEGUIR)

- Realizar revisiones periódicas a fin de determinar intromisiones de personal ajeno a la red o a equipos que no son de su competencia; así mismo, la revisión de los sucesos a los que es susceptible de auditar en cada uno de los equipos (auditar en horarios no usuales de uso para el propietario de la cuenta por medio del visor de sucesos).

- Revisar que el personal autorizado para cada equipo sea el que realmente haga uso del mismo (una forma de detección será por medio de los intentos que utiliza para entrar a la cuenta sin éxito).

- Revisar el grupo de trabajo que tiene asignado cada usuario para determinar si esto corresponde a los derechos de los cuales puede hacer uso, por medio de la descripción que presente el administrador de usuarios.

- Verificación de seguridad de directorios, así como los sucesos a auditar configurándose previamente como correcto o erróneo.

- Revisión periódica del visor de sucesos para ver que tipo de error se presento, así como en que equipo, la frecuencia y el origen.

RECOMENDACIONES GENERALES

- Los recursos de cómputo deben utilizarse en forma efectiva, mediante controles informáticos y adecuados y para lo cual se recomienda la asignación de un administrador de red dedicado que cumpla con las funciones especificas inherentes a dicha actividad para el mejor desempeño de actividades.

- Todas y cada una de las actividades encomendadas deben ser asignadas con responsabilidad al personal adecuado que así competa, de acuerdo a su experiencia y a sus aptitudes profesionales, para un mejor rendimiento y resultados revisando periódicamente por medio de un programa las cargas de trabajo para determinar si estas son terminadas oportuna y eficientemente en tiempo y forma.

- Examinar si las tareas asignadas, son acorde con los recursos con los que se cuenta, y si no es así, brindar las facilidades para que estos se puedan cumplir en un periodo de tiempo relativamente corto

- Tener especial control del lugar de cómputo en el cual se tienen los resguardos informáticos del Departamento y este segura en cualquier situación de siniestro o sabotaje.

- Realizar una bitácora informática con el ingreso y salida de los recursos informáticos (hardware y software) del Departamento.

- Tener mayor control sobre la información que se pone en la red para que únicamente sea copiada o utilizada por el usuario a quien va dirigida o bien con las restricciones adecuadas.

- Determinar y controlar el tipo de acceso que debe tener cada usuario con privilegios, permisos y accesos, ya que en general deben concederse los privilegios suficientes para cumplir con las tareas necesarias.

- Tener una lista documentada acerca de las restricciones de seguridad o de acceso en las que esta sujeto el usuario.

- Dada la necesidad de integrar sistemas de control administrativo para la mayoría de las actividades y necesidades de informática se plantea el requerimiento de personal especializado y dedicado a la creación, análisis y desarrollo de sistemas de tal forma que permita integrar rápidamente sistemas acorde a las actividades a controlar en cada una de las áreas permitiendo por un lado enriquecer y actualizar la información de las bases de datos con las que se cuenta y por otro lado desarrollar y mejorar estos sistemas.

- Realizar estudios de mejoras tecnológicas de hardware y software que beneficien el buen desempeño de las funciones informática-administrativas necesarias.

- Realizar un programa de capacitación de acuerdo al perfil de cada trabajador e intereses personales.

- Dar cursos de actualización a personal que tenga conocimientos medios o avanzados de computación a fin de romper con la dependencia de personas especializadas, así mismo de acuerdo a las necesidades prioritarias.

- Emigrar los programas de trabajo o software actualizado a fin de avanzar tecnológicamente y gradualmente a fin de lograr un buen acoplamiento a los nuevos sistemas.

- Lograr que se designe a un personal responsable del análisis y desarrollo de sistemas para que pueda concluir con los proyectos que se han quedado en la etapa de análisis.

- Organizar un grupo de trabajo para la buena administración de los recursos de cómputo y su mantenimiento (hardware y software) además del seguimiento del respaldo de información de cada equipo.

- Llevar el control de cambios o modificaciones a los sistemas, por medio de una bitácora por equipo de la red.

- Actualización de equipo informático con espacios no mayores a 4 años.

Riesgos latentes; podemos definir un riesgo como una amenaza que aprovecha un punto débil para dañar el sistema, al conocer los riesgos presentes, creando con esto directivas y planes para reducirlos.

Algunos procedimientos para reducir los riesgos que se deben considerar son los siguientes.

- Reunir al personal y levantar una sesión de aportación de lluvia de ideas de tal forma que enumeremos los activos y los riesgos para estos activos. (además de que ayude a crear conciencia con todo el personal).

- Actualización de evaluación de riesgos periódicamente, además de realizarlo en cada ocasión que se presente un cambio importante en la operación o estructura de la red, cambio de personal de directivas o algún otro cambio importante, así como alguna perdida potencial.

ALGUNAS MEDIDAS DE SEGURIDAD PREVENTIVAS

- Deberá de restringirse el uso del equipo de cómputo perteneciente a cada área y personal no calificado para hacer uso del mismo.
- Uso limitado a tareas propias del Departamento.
- Uso supervisado por el responsable del equipo, hacia el personal que colabore con el.
- Vacunar discos de dudosa procedencias o por prevención realizarlo en todos.
- No alterar configuraciones del sistema o alteraciones de archivos que sean desconocidos, esto se refiere al borrado de archivos, movimiento de carpetas, etc.
- No se deberá permitir instalar software que pudiese alterar configuraciones propias del sistema.
- Prohibir la instalación de juegos o de software no autorizado.
- Borrar archivos periódicamente que solo ocupan espacio provocando el alentamiento de la maquina, tal es el caso exclusivamente de los archivos con extensiones: TMP, CHK y ~.*

Con todas estas recomendaciones y acciones terminadas se pretende beneficiar en gran medida el correcto seguimiento y aplicación de las medidas preventivas reduciendo los riesgos latentes presentes llevando además controles y estadísticas en los cuales sea posible determinar claramente los avances y contar con el historial de problemáticas y soluciones propuestas, por lo cual se hace necesario el tener a una persona dedicada a la administración y seguridad informática para la red interna de los talleres la paz.

REALIZO

Susana Flores Leal

VISTO BUENO

Ing. Gerardo J. Chacón Cruz
Jefe del Departamento de Servicios de Mantenimiento al Material Rodante Férreo

CONCLUSIONES CAPITULO IV

Con la solución propuesta para apoyar el análisis, de desarrollo e implantación, acceso y control de la información, consulta de archivos, se comprueba que al hacer uso de la tecnología informática se logra integrar en forma significativa los procesos administrativos de información, además de incrementar la seguridad en el acceso de la misma.

El avance de la tecnología informática, permite aplicarla en cualquier ámbito; dando como resultados, mejor rendimiento en los equipos, reducción de tiempos, agilización en los procesos de trabajo, actualización oportuna de la información en el momento que esta sea requerida, con lo cual se establece que, el éxito de una empresa, depende en gran medida de la integración de la función informática así como en el buen desempeño de sus actividades y procesos, mejorando su agilización.

Con el manejo de la tecnología informática, se pueden mejorar notablemente los procesos y seguridad que muchas veces resultan complicados pero que con un buen desempeño de los recursos y estudio se logra que este sea la mejor solución y eficaz además de implantar la mejor solución.

A través de este proceso ha sido posible constatar, que aún a pesar de las deficiencias, es posible sacar ventajas de los recursos disponibles, ya que al analizar las circunstancias y riesgos es posible sacar provecho de ellos, de esta manera al ejecutar lo planeado en el paso que determinó la labor realizada, cualquier planteamiento es funcional en la manera en que se lleve a cabo de forma práctica, ya que si el planteamiento no se realiza debidamente, desde su ejecución, esta no funcionará.

En el siguiente capítulo, se planteará la etapa de documentación y seguimiento en el cual se contemplará un plan aprobado y un compromiso por parte del Jefe de Departamento para apoyar este proyecto.

CAPITULO V

DOCUMENTACION Y SEGUIMIENTO

CAPÍTULO V. ETAPA DE DOCUMENTACIÓN Y SEGUIMIENTO

En esta etapa, se tratará uno de los puntos más importantes, ya que se mencionaran cada uno de los pasos a seguir en el proceso de implantación de este proyecto, así como los principales problemas a los que se tuvo que enfrentar para realizarlo exitosamente.

En la etapa de seguimiento, compete al Jefe de Departamento y a los interesados, que la seguridad en informática se realice de forma continua y exitosa. La autorización y difusión del inicio del proyecto marca las normas para que todos los involucrados en la revisión participen y proporcionen información necesaria sobre los siguientes puntos:

- Determinar las debilidades que entorpecen la operación o generan improductividad durante los procesos.
- Se revisen los resultados obtenidos de la seguridad.
- Se definan líneas estratégicas para que las recomendaciones que generen acciones inmediatas, a mediano y largo plazo.
- Se faciliten los espacios y herramientas necesarias en la revisión del proyecto.
- Se establezcan los apoyos necesarios para que el personal a su cargo se comprometa a llevar a cabo las acciones recomendadas en el informe final.

Una vez terminado el proceso de seguridad, es conveniente programar revisiones periódicas que aseguren que el personal de la empresa está llevando a cabo una correcta explotación de los recursos informáticos y se deben programar visitas a las áreas más importantes que se hayan evaluado para comprobar, el cumplimiento formal de los procedimientos en tiempos y formas programados, así como documentar loas debilidades y anomalías mas relevantes, posteriores a la implantación.

Al momento de iniciar con este proyecto denominado "Seguridad Informática en los Talleres la Paz del Sistema de Transporte Colectivo Metro", este se realizo con la idea de analizar la seguridad existente actual e implantar los mejores métodos de protección para tener una buena seguridad, no solo basta con desarrollarlos, sino adaptarlos a las necesidades de la organización considerando los puntos más débiles de la red y sistemas instalados, así como la información a proteger y los usuarios.

Para ello se desarrollo en este proyecto un plan de seguridad ajustándolo a los requerimientos necesarios a fin de sistematizar y aplicar de una forma ordenada las medidas de protección contra los diferentes tipos de amenazas realizando un análisis de manera integral del estado actual de la seguridad adaptando las mejoras correspondientes y realizando revisiones periódicas sin perder de vista que esta debe convertirse en algo útil y fácil de implementar.

Para ello se considera conveniente que exista un responsable definido para llevar a cabo la seguridad, porque a pesar de que existan diferentes categorías y grados de responsabilidad, en ocasiones no se define quien es el responsable de la misma. A menudo sucede que no hay una directriz bien definida y la información se dispersa entre todos los usuarios, y con esto no se logran soluciones prontas cuando suceda algún incidente, ya que cuando más difusa es una responsabilidad, se vuelve más complicada la coordinación de funciones y existen menos posibilidades de que se lleve a cabo con resultados exitosos. Es por ello que se considera necesario asignarse a una persona especifica esta responsabilidad, cuya tarea principal sea la

supervisión constante del estado de la seguridad, para que sea el indicado de que en cuanto ocurra un incidente de seguridad este lo resuelva, tratándose desde una detección de virus o cualquier problema mayor de intrusión a la seguridad que se presente. Así los demás usuarios sabrán a quien recurrir y de esta manera resulta más fácil hacer llegar sus consultas y habrá más posibilidades de que la implantación de medidas y sistema de seguridad resulten satisfactorias, de esta manera las tareas de seguridad dejarán de estar dispersas entre todos sus integrantes, y así será posible aplicar la seguridad de forma más adecuada, consistente y uniforme.

Una de las principales tareas ha sido la identificación de los puntos clave, es decir toda aquella información y sistemas que para la empresas tengan un gran valor y que por lo tanto se deban proteger, como pueden ser bases de datos, programas de mantenimiento, procedimientos de trabajo, información técnica o confidencial sobre garantías del proveedor o bien, actividades propias de la empresa o desarrollo en investigaciones o nuevos proyectos. Para garantizar el orden de importancia es conveniente se cataloguen de mayor a menor importancia por orden de prioridad.

Aún así no sólo basta con ello, si no que además deberán tenerse de manera muy clara cuales son los peligros a los que están expuestos y que puedan afectarlos. La mejor forma de hacerlo es realizando una segunda lista para los diferentes riesgos y vulnerabilidades que podrían poner en peligro la seguridad, como podrían ser virus, gusanos, ataques de negación de servicio, alteración de información, robo de archivos, intrusión a los equipos, equipos portátiles etc., es muy importante clasificarlos de más a menos críticos, para la seguridad.

Uno de los objetivos que al igual de los demás se considera importante es la Gestión de Riesgos, esto se refiere a la evaluación del riesgo que cada vulnerabilidad o amenaza supone para los puntos clave, teniendo en cuenta que deben establecerse prioridades al momento de establecer estrategias de seguridad.

A fin de realizar una correcta protección de los diferentes puntos clave es importante marcar una clara estrategia de seguridad que sea coherente, con las prioridades de protección de los recursos, para ello deberá realizarse un listado ordenando de mayor a menor necesidad de protección, pero además deben de tomarse en cuenta las políticas que se encuentren vigentes en la empresa, para así saber como aplicar y configurar las diferentes tecnologías y sistemas de seguridad y además estas no deben afectar negativamente los procesos de producción. Por consiguiente deben realizarse procedimientos que definan como aplicar en la práctica las políticas de seguridad, así como que acciones hay que realizar en caso de producirse un incidente de seguridad.

Es importante recalcar que las políticas y procedimientos deben abarcar todas las áreas de seguridad tratadas entre ellas,. Correo electrónico, internet, descarga e instalación de programas, uso y configuración de pc's lap tops, pasword, vigilancia de usuarios, privacidad, asignación de tareas de seguridad, respuesta ante incidencias, firewalls, encriptación, firmas digitales, transferencias de datos y comunicaciones, acceso remoto y antivirus.

Además de esto el siguiente paso es el realizar la implementación de medidas de acuerdo con las estrategias desarrolladas, no obstante, es necesaria una cierta capacidad de improvisación, ya que siempre surgen novedades y cambios de última hora por lo cual no siempre es posible seguir reglas establecidas, para lo cual debe existir cierto grado de flexibilidad.

Para ello, una vez que se ha considerado el proceso de implementación y se ha llegado a su funcionamiento, hay que asegurarse que realmente cumplan los procedimientos, es por ello que se vuelve necesario realizar un seguimiento continuo, este seguimiento tiene dos finalidades.

La primera comprobar una correcta integración de las medidas y políticas con las últimas rutinas de trabajo de la empresa, evitando así que interrumpa en los diferentes procesos laborales y productivos.

Segundo comprobar que realmente se adecuan a las prioridades y que evitan amenazas, ataques y vulnerabilidades.

Toda estrategia de seguridad que esté bien realizada, debe contar con 3 pilares denominados tecnología, política y formación, esto último es vital para que la protección informática sea exitosa; puesto que los usuarios son quienes van a beneficiarse directamente de esta protección.

Realmente hay que contar con los usuarios para que la seguridad funcione, para ello, es necesario la formación ya que tienen para familiarizarse con las nuevas políticas de seguridad y lo que es más importante, deben entender la importancia de la protección y la seguridad, lo que en ocasiones esto es precisamente lo que se vuelve más complicado.

No obstante, es muy importante entender que las medidas de seguridad y protección no duran eternamente. La seguridad es dinámica, cambia con rapidez y la empresa tiene que estar siempre actualizada al día, para evitar convertirse en una víctima de los hackers, virus u otras amenazas. Los riesgos y las amenazas evolucionan, se sofistican con una rapidez terrible. Por ello, las tecnologías de seguridad también cambian a gran velocidad haciéndose cada vez más eficaces.

Todo esto ha sido el proceso, llevado a cabo para completar este proyecto de Seguridad informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro, pero además como un último punto para no quedar desfasados y evitar el riesgo de ataques, es conveniente que cada semestre se deberá proceder a una revaloración de las estrategias políticas y prioridades. Esto no significa que cada seis meses se deban cambiar de nuevo todas las tecnologías de seguridad, sino que algunas se deberán actualizarse y otras tan solo deben ser revisadas y ajustarse en caso de ser necesario.

PLAN APROBADO Y COMPROMISO

El éxito de cualquier política gerencial requiere del compromiso explícito e implícito de la alta gerencia. La seguridad computacional no es la excepción, los proyectos que han triunfado se caracterizan todos por contar con un alto grado de compromiso por parte de la Empresa, además de la dedicación profesional del personal integrante de las áreas de informática, para garantizar la obtención de resultados efectivos en cuanto a seguridad de la información y los recursos se refiere.. La Empresa también debe estar reforzada por la evidencia tangible de la presencia de mecanismos y procedimientos establecidos de seguridad; las tarjetas de identificación y control de accesos electrónicos o magnéticos, o algún otro medio de seguridad deben estar plenamente considerados en la protección de los recursos informáticos. (anexo No. 4)

EJECUTAR PERIODICAMENTE LOS PROCEDIMIENTOS APROBADOS Y DOCUMENTADOS

Para poder establecer los criterios necesarios y analizar si los procedimientos han sido lo suficientemente productivos, se tendrán que considerar en conjunto los resultados obtenidos poniendo especial atención en la revisión de los objetivos planeados.

La observación en los resultados será, a fin de poder mejorar en un futuro y con ello poder tomar las decisiones acertadas a fin de mejorar cada vez en los controles y toma de decisiones posteriores, así mismo si las técnicas y métodos empleados han sido eficaces para la obtención de los objetivos, contribuyendo positivamente en la Seguridad Informática llevada a cabo.

Por otro lado también es de suma importancia establecer lineamientos para poder dar seguimiento a los usuarios y a los tipos de seguridad que se pretender salvaguardar.

Considerándose que estas actividades deben satisfacer las necesidades de cada coordinación esta debe de ser una actividad dinámica que no puede limitarse a realizarse una ocasión sino que debe continuar a fin de retroalimentar y mejorarse en cada suceso que se presente.

Para esto es importante documentar un programa de seguimiento el cual debe contener.

- Facilidad de adaptabilidad a nuevas necesidades.
- Flexibilidad de programas de trabajo a situaciones generales y particulares.
- Evaluación periódica de sucesos.
- Control estadístico de resultados obtenidos.
- Comunicación permanente con los usuarios

CONCLUSIONES CAPITULO V

Para poder lograr la implementación y una correcta evaluación de riesgos se detectaron que existen debilidades y vulnerabilidades en los controles de seguridad, debido a la falta de seguridad y al factor humano insuficiente, pero con frecuencia las directivas demasiado rigurosas se pasan por alto porque las personas ya no desean cumplirlas, lo cual provoca puntos débiles en las brechas y en los ataques a la seguridad, para lo cual se pretende avanzar gradualmente y así lograr una completa implementación y control de los recursos, con un grado de flexibilidad adecuado.

En el estudio de campo que se realizó por medio de cuestionarios, encuestas, entrevistas, fue fácil detectar los errores en los que incurre normalmente el personal, ya que no existen medidas y políticas de seguridad bien definidas, pero con el presente estudio se han detectado, analizado y corregido en la medida de las posibilidades y recursos actuales sin alterar los procesos de trabajo, de la empresa además de previa aprobación por parte de usuario.

Para la realización del análisis de la directiva de seguridad se considero de acuerdo con la posibilidad de pérdida o divulgación en las siguientes categorías de información, además de requisitos de manipulación independientes como; importantes, confidencial, privada y pública las cuales las definimos de la siguiente manera.

Importante; Esta se considero para la información que necesita estar protegida contra modificación o eliminación no autorizadas de tal forma que se logre asegurar su integridad y en la cual la seguridad debe ser más alta que la normal.

Confidencial; La cual es utilizada dentro del Departamento y para la cual su divulgación no autorizada podría afectar seriamente las políticas e intereses de la Empresa.

Privada; Esta se refiere a información personal que se utiliza dentro del Departamento y a la cual su divulgación puede afectar al mismo, o a algún empleado.

Pública; Esta es para cualquier información que no cae en ninguna de las clasificaciones anteriormente mencionadas y es importante que el personal la conozca.

CONCLUSIONES GENERALES

Durante el desarrollo del presente trabajo se adquirió experiencia de gran importancia complementando con esto la formación profesional adquirida, como resultado de estos conocimientos a continuación se presenta el análisis de las principales ideas, inquietudes, problemáticas y logros obtenidos.

Al realizar el proyecto de Seguridad en informática en los Talleres La Paz del STC- Metro (de la red informática interna del departamento) se puede constatar que el buen uso de lineamientos y recursos reducen los riesgos de pérdida de información, sabotaje o intrusión a los mismos, logrando con ello una máxima eficiencia en el desarrollo de las actividades realizadas, ahorrando significativamente a la Empresa tiempo, dinero y derroche de recursos innecesariamente.

Por otra parte, es importante comentar las dificultades enfrentadas durante el proceso del proyecto para comprender y considerar el trabajo de análisis, desarrollo y problemática que le dieran origen; para ello a continuación se mencionan algunas de las principales dificultades presentadas.

La mayor dificultad que se presentó fue la falta de tiempo que tenía el personal usuario para llenar los cuestionarios y en otras ocasiones para considerar y responder a ciertos aspectos técnicos, siendo que el personal no cuentan con los conocimientos en informática necesarios, motivo por el cual se tuvo que realizar un intenso trabajo de convencimiento y concientización de la importancia que tiene la seguridad informática para la Empresa y en el desarrollo de sus múltiples actividades, pero debido a las circunstancias expuestas, se tomó la determinación de trabajar en forma conjunta con los usuarios a lo largo de todo el desarrollo del proyecto, de esta forma involucrarlos en el proceso de cambio hacia la implementación de los mecanismos físicos y lógicos de seguridad en los equipos.

Otro problema que se tuvo fue por las diferentes actividades que realiza el personal y en ocasiones horarios variables, debido a las múltiples actividades y cargas de trabajo por lo cual había que ajustarse a sus tiempos, provocando con esto el atraso en el proceso de estudio y análisis, pero era importante saber la forma de trabajo de cada uno de los usuarios y al mismo tiempo ver los procesos, las actividades que cada uno opera, de esta forma permitiendo generar más fácilmente la información necesaria para continuar con el desarrollo, y en un futuro facilitar el manejo y mantenimiento de los equipos. En ocasiones no se sigue con la metodología establecida, por cuestiones generalmente de premura de tiempo, lo que repercute en el desarrollo. En la práctica resultan de gran utilidad sus puntos de vista, para tener una perspectiva clara de todos los procesos, las responsabilidades de cada uno de los usuarios y en general todo el proceso de compartición de información, permisos, privilegios de acuerdo a las áreas que controlan y la información que se genera.

Al realizar este trabajo se ha logrado un ahorro en gastos directamente a la Empresa, en beneficio del presupuesto y del gasto público, condicionalmente si se hubiera contratado a un especialista para determinar el grado de seguridad y las acciones a tomar implicaría hacer uso de los recursos económicos, de esta manera se obtuvo la experiencia además de tener como beneficio, optimizar los recursos y reducir considerablemente las fallas, lo cual ahora con la cantidad de trabajo existente por la adquisición de nuevos proyectos, además de que no siempre existían personas con cultura informática adecuada, de tal manera que el contar con su apoyo permitió que los usuarios se identificaran y ayudaran en la investigación de campo, por lo tanto la seguridad en informática es un proyecto importante que debe considerarse para el buen funcionamiento de los servicios de manejo de datos, seguridad de la información y así mismo para los usuarios de la red, la cual servirá para garantizar la continuidad de las operaciones, porque de no considerarse y no darle la importancia debida se corre el riesgo de perder información valiosa e histórica de controles

administrativos, programas de mantenimiento, procedimientos de trabajo, programas y aplicaciones informáticas, afectando gravemente en su desarrollo. Es por ello que este Proyecto de Seguridad Informática en los Talleres la Paz requiere darle la importancia debida, con los apoyos necesarios de soporte, equipos e infraestructura que ayuden a fortalecer todas y cada una de las actividades que se desarrollarán en el mismo, por lo tanto todo lo aquí planteado es conveniente llevarlo a cabo y darle un eficiente seguimiento, para garantizar siempre su buen funcionamiento. De esta manera los planteamientos expuestos nos brindan las herramientas necesarias de proceso para tener una mayor seguridad y mejor control de los equipos informáticos y de la propia información.

Es recomendable lograr establecer un comité formal de seguridad computacional, el cual deberá asumir la responsabilidad, de coordinar la revisión en el momento oportuno de manera regular y sorpresiva, así como también de realizar la acción apropiada. El hecho de que el comité de seguridad se reúna de manera regular, garantiza el seguimiento periódico de las actividades y por ende, no olvidarse con el paso del tiempo.

GLOSARIO

ANALISTA DE SISTEMAS: Persona capacitada en la definición y el análisis de problemas, la cual examina una situación comercial o industrial y diseña un sistema de cómputo que cubra las necesidades de información y operación.

ARCHIVO: Colección de datos sobre una o varios temas relacionados, la cual se maneja como una sola entidad.

SEGURIDAD: Pasos diseñados con el fin de confirmar las evidencias relacionadas con la autenticidad y validez de los datos en un sistema de procesamiento de datos.

BASE DE DATOS: Colección compartida de datos interrelacionados diseñados para cubrir las necesidades de muchos tipos de usuarios.

CAPTURA DE DATOS: Obtención de datos mediante un dispositivo que se pueda comunicar con un sistema de cómputo

CONTROL: Función construida dentro de un programa como mecanismo de verificación.

DATOS: En la terminología de computación, los hechos, la información o los caracteres que procesa, almacena o produce una computadora.

DISCO: Placa delgada circular cubierta con material magnético, en la cual se graban y almacenan los datos. Los discos son básicamente de dos tipos: duros y flexibles, Los duros tienen una base de metal o de vidrio; los flexibles son de plástico.

DOCUMENTACIÓN: Descripción de las funciones de un programa, o grupo de programas, o un sistema.

EQUIPO (Hardware): Dispositivos de procesamiento de datos donde se incluye el sistema de cómputo –principal, mini, o micro- y el equipo periférico, como las terminales e impresoras de línea.

INTERFASE: Punto de interacción entre dos sistemas o procesos.

PREPARACIÓN DE DATOS: Registro de los datos por medio de un dispositivo de entada como preparación del suministro para una computadora.

PROCESAMIENTO DE DATOS: Disposición de los datos en cierta forma que produzcan resultados deseados; el manejo de los datos para su clasificación, ordenamiento cálculo y registro; la producción y actualización de registros e informes.

PROGRAMA: Serie de instrucciones que indican a la computadora como realizar una tarea especifica.

TERMINAL: Dispositivo mediante el cual el usuario se comunica con la computadora. Se trata de un recurso de entrada y salida, que consiste en un tablero, una pantalla y/o una impresora. También puede incluir un microprocesador y recurso de programación.

LEGISLACIÓN

ASPECTOS JURÍDICOS DE LOS DELITOS COMPUTACIONALES

El gran aumento de los delitos computacionales ha hecho evidente la necesidad de aplicar leyes con base en la magnitud alcanzada por la tecnología de la computación.

Actualmente la Ley Federal del Derecho de Autor, vigente en México, incluye en el Título IV capítulo IV, un apartado sobre la Protección del Derecho de Autor, en lo que a programas de computación y Base de datos se refiere, se exponen en seguida los artículos a los que se hace referencia.

TITULO IV VAPITULO IV Ley federal del derecho de Autor; De los Programas de Computación y las Bases de Datos.

ART. 101: Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

ART. 102: Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.

ART. 103: Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a éste.
Como excepción a lo previsto por el artículo 33 de la presente Ley, el plazo de la cesión de derechos en materia de programas de computación no está sujeto a limitación alguna.

ART. 104: Como excepción a lo previsto en el artículo 27 fracción IV, el titular de los derechos de autor sobre un programa de computación o sobre una base de datos conservará, aún después de la venta de ejemplares de los mismos, el derecho de autorizar o prohibir el arrendamiento de dichos ejemplares. Este precepto no se aplicará cuando el ejemplar del programa de computación no constituya en sí mismo un objeto esencial de la licencia de uso.

ART. 105: El usuario legítimo de un programa de computación podrá realizar el número de copias que el autorice la licencia concedida por el titular de los derechos de autor, o unas sola copia de dicho programa siempre y cuando:

I.- Sea indispensable para la utilización del programa, o
II.- Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho de usuario para utilizar el programa de computación.

ART. 106: El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir;

I.- La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma;
II.- La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante;
III.- Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler, y
IV.- La decompilación, los procesos para revertir la ingeniería de un progama de computación y el desensamblaje.

ART. 107: Las bases de datos o de otros materiales legibles por medio de máquinas o en otra fora, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en si mismos.

ART. 108: Las bases de datos que no sean originales quedan, sin embargo, protegidas en su uso exclusivo por quien las haya elaborado, durante un lapso de 5 años.

ART. 109: El acceso a la información de carácter privado relativa a las personas contenida en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.
Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.

ART. 110: El titular del derecho patrimonial sobre una base de datos tendrá el derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorizar o prohibir:

I.- Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma;
II.- Su traducción, adaptación, reordenación y cualquier otra modificación;
III.- La distribución del original o copias de la base de datos;
IV.- La comunicación al público, y
V.- La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.

ART 111: Los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados quedan protegidos por esta Ley en los elementos primigenios que contengan.

ART. 112: Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior.

ART. 113: Las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de está transmisión estarán protegidas por esta ley.

ART.114: La transmisión de obras protegidas por esta ley mediante cable, ondas radioeléctricas, satélite u otras similares, deberán adecuarse, en lo conducente, a la legislación mexicana y respetar en todo caso y en todo tiempo las disposiciones sobre la materia.

INFORMACIÓN TOMADA Pierre Gratton, Protección Informática Editorial trillas, año 1988

Bibliografía

Seguridad de Centros de Cómputo, Objetivos, Lineamientos y Procedimientos.
Autor: David H. Li
Editorial: Trillas 1992
Total de Páginas: 176
México D.F

Informática Presente y Futuro
Autor: Sanders. Donald H.
3a Edición
Editorial: Mc Graw Hill 1990
Total de Páginas: 887
México D.F

Sistemas de Información por Computadora Metodología de Desarrollo.
Autor: Juan Manuel Márquez Vite.
Editorial: Trillas
1ª. Edición Octubre de 1987
Total de Páginas: 218

Derecho Informático.
Autor: Julio Téllez Valdez
(Instituto de Investigaciones Jurídicas Serie G Estudios Doctrinales No. 102)
1a Edición Abril de 1987
Total de páginas: 247
Universidad: UNAM.

Computer -Security and Technology
Autor: James Arlin Cooper
1984 SEG. IMP. Octubre Publicada en Canadá y EUA
Total de páginas 167

Secure Computers and Networks, Design, and Implementation
Autores: Erick A. Fisch, Pn. D. Gregori B. White, Ph. D.
Editorial: CR Press Año 2000
Boca Raton, Florida.
Total de Páginas: 370

Seguridad en Centros de Cómputo Políticas y Procedimientos.
Autor: Leonard H. Fine
Editorial: Trillas
1a Edición Abril de 1988, México D.F
Total de páginas: 129

Todo acerca de redes de computación
Autor: Kevin Stoltz
Traducción: Ing. Sergio Luis, María Ruiz Faudon
Ing. Químico Universidad Veracruzana
Editorial: Prentice may Americava, S.A.
Impreso en México 1995
Total de páginas: 517

Informática 3ª. Edición
Autores: Wilson T. Price Merritt Collage
Oaklad, California
Traducción: Agustín Cantín Sanz
Nueva Editora Interamericana S.A. de C.V. 1985
Mexico D.F. 2ª. Reimp. 1984

Protección Informática
Autores: Pierre Gratton
México
Editorial Trillas
Mexico D.F. 2ª. Reimp. 1998

ANEXOS

ANEXOS 1

Análisis de Fuerzas, Oportunidades, Debilidades y Amenazas

ANÁLISIS DE FUERZAS OPORTUNIDADES, DEBILIDADES Y AMENAZAS(FODA) EN EL ÁREA DE INFORMÁTICA EN TALLERES LA PAZ.

NOMBRE DEL USUARIO: _____ **FECHA:** ___/___/02

ÁREA DE TRABAJO: _____ **NÚMERO DE NODO:** _____

Este análisis tiene la finalidad de identificar las **circunstancias internas** que influyen en el área de informática representadas por:

FUERZAS con las que se cuenta entendiendose por estas como todas aquellas características con las que actualmente cuenta y que favorecen al área informática.

Debilidades que usted observe como carencias y deficiencias.

Así mismo se identificarán aquellas **causas externas** que afectan a la unidad informática constituidas por:

Amenazas como lo son el mal uso de la información, mal manejo de equipo etc.

Oportunidades que usted cree convenientes para un mejor aprovechamiento de los recursos informáticos.

Al final lo que se busca es convertir estas debilidades en oportunidades y las amenazas en fuerzas

INSTRUCCIONES: Llene cada uno de los recuadros según tu opinión y experiencia con los equipos.

FUERZAS	AMENAZAS
Existencia de antivirus en todos los equipos informaticos para evitar la contaminacion con algún virus presente	Realizacion de algun cambio físico en los equipos sin conocimientos previos Mal uso de la información al no contar con las contraseñas para cada equipo
DEBILIDADES	**OPORTUNIDADES**
- Situaciones de bloqueo por la sola existencia de un unico administrador y que no pueden darse de alta usuarios o cambiar algun dato en el servidor - Falta de una bitacora de trabajo para cada uno de los nodos y el servidor mismo - El no contar con respaldos en discos magneticos aumenta el riesgo de sufrir perdida de información importante	

ANÁLISIS DE FUERZAS OPORTUNIDADES, DEBILIDADES Y AMENAZAS(FODA) EN EL ÁREA DE INFORMÁTICA EN TALLERES LA PAZ.

NOMBRE DEL USUARIO: JONATHAN E. PEÑA BALSERO **FECHA:** 15/01/02
ÁREA DE TRABAJO: C.C.I.T.A. **NÚMERO DE NODO:** CITA

Este análisis tiene la finalidad de identificar las circunstancias internas que influyen en el área de informática representadas por:

FUERZAS con las que se cuenta entendiendose por estas como todas aquellas características con las que actualmente cuenta y que favorecen al área informática.

Debilidades que usted observe como carencias y deficiencias.

Así mismo se identificarán aquellas **causas externas** que afectan a la unidad informática constituidas por:

Amenazas como lo son el mal uso de la información, mal manejo de equipo etc.

Oportunidades que usted cree convenientes para un mejor aprovechamiento de los recursos informáticos.

Al final lo que se busca es convertir estas debilidades en oportunidades y las amenazas en fuerzas

INSTRUCCIONES: Llene cada uno de los recuadros según tu opinión y experiencia con los equipos.

FUERZAS	AMENAZAS
FACILITA EN GRAN MANERA LA LOCALIZACION DE DATOS Y ESTA CA COMO RESULTADO UN ACCESO CORRECTO Y MUCHA EFICIENCIA	UNA DE ESTAS ES QUE ALGUNO PUEDA INTRODUCIR UN DISCO CON VIRUS Y CAUSE EL COLAPSO DEL SISTEMA INFORMATICO CONFIDENCIAL QUE PUEDE SER UTILIZADA PARA FINES PERSONALES O LA IMPOSIBILIDAD DE ACCESO A LA INFORMACION

DEBILIDADES	OPORTUNIDADES
SE A DUELTO EL EQUIPO DEMASIADO LENTO AL INTENTAR ABRIR O CARGAR ALGUN ARCHIVO O PROGRAMA O CONSTANTEMENTE SE TIENEN PROBLEMAS PARA CONECTARSE A LA RED	ESTO QUE ES NECESARIO QUE SE LES DE MANTENIMIENTO SEGUIDO YA QUE EL EQUIPO SE ENCUENTRA EN UN AREA DE MUCHO POLVO Y ESTO HACE QUE EL EQUIPO ASI COMO TAMBIEN ACTUALIZAR LA PAQUETERIA YA QUE CON EL TIEMPO SE VUELVE OBSOLETO.

ANÁLISIS DE FUERZAS OPORTUNIDADES, DEBILIDADES Y AMENAZAS(FODA) EN EL ÁREA DE INFORMÁTICA EN TALLERES LA PAZ.

NOMBRE DEL USUARIO: Rogelio Aquino F. **FECHA:** 14/02/02
ÁREA DE TRABAJO: Mantto. Hdwar **NÚMERO DE NODO:** 01

Este análisis tiene la finalidad de identificar las **circunstancias internas** que influyen en el área de informática representadas por:

FUERZAS con las que se cuenta entendiendose por estas como todas aquellas características con las que actualmente cuenta y que favorecen al área informática.

Debilidades que usted observe como carencias y deficiencias.

Así mismo se identificarán aquellas **causas externas** que afectan a la unidad informática constituidas por:

Amenazas como lo son el mal uso de la información, mal manejo de equipo etc.

Oportunidades que usted cree convenientes para un mejor aprovechamiento de los recursos informáticos.

Al final lo que se busca es convertir estas debilidades en oportunidades y las amenazas en fuerzas

INSTRUCCIONES: Llene cada uno de los recuadros según tu opinión y experiencia con los equipos.

FUERZAS	AMENAZAS
Disponibilidad de archivos generados por otros usuarios para agilizar el movimiento de información. Guardar archivos de importancia o de interés para otras áreas en el Servidor o que sirven para respaldo informático. Disponibilidad ocasional para enviar atraves de la red impresiones.	Virus informáticos en la red o que pudieran infectar áreas terminales. Implementar claves de usuarios para el acceso a la red o evitar mal uso de la información por personas no autorizadas.
DEBILIDADES	**OPORTUNIDADES**
Material de Hardware obsoleto en las terytas o computadoras. Ocasionalmente no es posible acceder al Servidor.	Disponibilidad de toda la información atraves del servidor de todas las terminales en red las 24 hrs. los 365 días del año. Disponibilidad informática para vacunar todas las terminales cada semana o evitar perdida de archivos atraves de la red. Disponibilidad total para enviar impresiones de los archivos durante las horas de servicio del área de informática.

ANÁLISIS DE FUERZAS OPORTUNIDADES, DEBILIDADES Y AMENAZAS(FODA) EN EL ÁREA DE INFORMÁTICA EN TALLERES LA PAZ.

NOMBRE DEL USUARIO: _____ **FECHA:** ___/___/02

ÁREA DE TRABAJO: _____ **NÚMERO DE NODO:** _____

Este análisis tiene la finalidad de identificar las **circunstancias internas** que influyen en el área de informática representadas por:

FUERZAS con las que se cuenta entendiendose por estas como todas aquellas características con las que actualmente cuenta y que favorecen al área informática.

Debilidades que usted observe como carencias y deficiencias.

Así mismo se identificarán aquellas **causas externas** que afectan a la unidad informática constituidas por:

Amenazas como lo son el mal uso de la información, mal manejo de equipo etc.

Oportunidades que usted cree convenientes para un mejor aprovechamiento de los recursos informáticos.

Al final lo que se busca es convertir estas debilidades en oportunidades y las amenazas en fuerzas

INSTRUCCIONES: Llene cada uno de los recuadros según tu opinión y experiencia con los equipos.

FUERZAS	AMENAZAS

DEBILIDADES	OPORTUNIDADES

ANÁLISIS DE FUERZAS OPORTUNIDADES, DEBILIDADES Y AMENAZAS(FODA) EN EL ÁREA DE INFORMÁTICA EN TALLERES LA PAZ.

NOMBRE DEL USUARIO: Justino A García L. **FECHA:** 20/02/02
ÁREA DE TRABAJO: [illegible] **NÚMERO DE NODO:** CSMR6

Este análisis tiene la finalidad de identificar las **circunstancias internas** que influyen en el área de informática representadas por:

FUERZAS con las que se cuenta entendiendose por estas como todas aquellas características con las que actualmente cuenta y que favorecen al área informática.

Debilidades que usted observe como carencias y deficiencias.

Así mismo se identificarán aquellas **causas externas** que afectan a la unidad informática constituidas por:

Amenazas como lo son el mal uso de la información, mal manejo de equipo etc.

Oportunidades que usted cree convenientes para un mejor aprovechamiento de los recursos informáticos.

Al final lo que se busca es convertir estas debilidades en oportunidades y las amenazas en fuerzas

INSTRUCCIONES: Llene cada uno de los recuadros según tu opinión y experiencia con los equipos.

FUERZAS	AMENAZAS
- Disponibilidad casi inmediata de la información capturada en las diferentes maquinas de la red. - Acceso en red a otras maquinas para consulta de otras [illegible]	- Falta de un control de accesos a la red eficiente - Falta de un archivo de claves en común acuerdo con el área de control - Herramientas de Mantenimiento para el servidor - Asignación de espacio en servidor con un alto control y seguridad por los usuarios. - Respaldos actualizados o programados a fin de mantener la integridad de los mismos. - Fácil ataque con virus o Hacker
DEBILIDADES	**OPORTUNIDADES**
- Entradas muy fáciles de los nodos a toda la Información de la red. - No jerarquizar los accesos - No haber catálogo de [illegible]	- Capacitar a los usuarios conforme nivel de uso de la red - Verificación periódica de todos los nodos y usuarios conforme programa - Mayor control de accesos - Verificación del uso de Windows y [redacted] porque tenía acceso a las [illegible] - Listado de uso de cada uno de las maquinas y responsables

- Requiere más tamaño de renglón
- Más precisión en la explicación de c/u de los puntos solicitados y debidamente definidos. (no mezclados)

ANÁLISIS DE FUERZAS OPORTUNIDADES, DEBILIDADES Y AMENAZAS(FODA) EN EL ÁREA DE INFORMÁTICA EN TALLERES LA PAZ.

NOMBRE DEL USUARIO: Medina Garcés Sandra A. **FECHA:** 22/03/02

ÁREA DE TRABAJO: Coordinación del área de Servicios **NÚMERO DE NODO:** CSUA-3

Este análisis tiene la finalidad de identificar las **circunstancias internas** que influyen en el área de informática representadas por:

FUERZAS con las que se cuenta entendiendose por estas como todas aquellas características con las que actualmente cuenta y que favorecen al área informática.

Debilidades que usted observe como carencias y deficiencias.

Así mismo se identificarán aquellas **causas externas** que afectan a la unidad informática constituidas por:

Amenazas como lo son el mal uso de la información, mal manejo de equipo etc.

Oportunidades que usted cree convenientes para un mejor aprovechamiento de los recursos informáticos.

Al final lo que se busca es convertir estas debilidades en oportunidades y las amenazas en fuerzas

INSTRUCCIONES: Llene cada uno de los recuadros según tu opinión y experiencia con los equipos.

FUERZAS	AMENAZAS
Como la elaboración de formatos en Word o Excel. Creación de fórmulas. Configuración del equipo como su mismo desempeño	Que el personal no sepa usarlo y solo mueva ocasionando una desconfiguración. O que el equipo solo sea usado para meter juegos que disminuya el rendimiento del equipo.
DEBILIDADES	**OPORTUNIDADES**
Que el equipo no sea el óptimo y sin el mayor elaboración de las fórmulas	Que les dé a conocer la capacidad de las fórmulas para una mejor optimización del equipo

ANÁLISIS DE FUERZAS OPORTUNIDADES, DEBILIDADES Y AMENAZAS(FODA) EN EL ÁREA DE INFORMÁTICA EN TALLERES LA PAZ.

NOMBRE DEL USUARIO: PEREZ MTZ ERICK JORGE **FECHA:** 22/02/02
ÁREA DE TRABAJO: Coordinación del área de [illegible] **NÚMERO DE NODO:** COMP-3

Este análisis tiene la finalidad de identificar las **circunstancias internas** que influyen en el área de informática representadas por:

FUERZAS con las que se cuenta entendiendose por estas como todas aquellas caracteristicas con las que actualmente cuenta y que favorecen al área informática.

Debilidades que usted observe como carencias y deficiencias.

Así mismo se identificarán aquellas **causas externas** que afectan a la unidad informática constituidas por:

Amenazas como lo son el mal uso de la información, mal manejo de equipo etc.

Oportunidades que usted cree convenientes para un mejor aprovechamiento de los recursos informáticos.

Al final lo que se busca es convertir estas debilidades en oportunidades y las amenazas en fuerzas

INSTRUCCIONES: Llene cada uno de los recuadros según tu opinión y experiencia con los equipos.

FUERZAS	AMENAZAS
Las Fuerzas en las computadoras son los software que nos como usuario [illegible] para tener mas rapidez en los trabajos.	Las amenazas que podemos encontrar en los equipos son los virus que tendremos que eliminar.

DEBILIDADES	OPORTUNIDADES
Las debilidades son defectos que tienen la computadora y que [illegible] las empresas [illegible]	Las oportunidades que podemos encontrar en los equipos son el aprendizaje que podemos tener en la computadora.

ANEXO 2

Cuestionario Diagnóstico

Etapa Preliminar de Seguridad Informática en los Talleres la Paz del S.T.C.

Cuestionario de diagnóstico actual
"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

Este cuestionario tiene la finalidad de conocer a grandes rasgos el estado en el que se encuentran los Sistemas y Equipos Informáticos utilizados para las diferentes actividades de las áreas del Taller.

A) Soluciones de Informática (.Diagnóstico de los Talleres La Paz).

Instrucciones: Marque con una cruz en los recuadros la respuesta que crea usted más conveniente de acuerdo a su criterio.

Servicios	Calificación en base al grado de satisfacción			
	Excelente	Bueno	Regular	Deficiente
• **Soluciones de consultoría** Asesoría, apoyo técnico y soporte presentado por el apoyo informático en la evaluación y solución de problemas presentados	( )	( )	X	( )
• **Soluciones de sistematización y capacitación en procesos** En la instalación de sistemas requeridos en el desarrollo de sus funciones operativas, tácticas y estratégicas	( )	X	( )	( )
• **Soluciones de desarrollo tecnológico** Evaluación y selección de tecnología de vanguardia;	( )	( )	( )	X
• **Servicios operativos** · Instalación de equipo de cómputo y telecomunicaciones · Capacitación en el uso de la tecnología · Atención a fallas de software y aplicaciones · Atención a fallas en equipos de cómputo y comunicaciones	( )	( )	X	( )

B) Sistemas de información instalados "diagnostico de informática"

INDICACIONES Contestar sólo por los conductores de los trenes.	Si	No
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	( )
Sistemas operativos de información Nombre (s) –Nivel Técnico.	( )	( )

C) Software instalado "Diagnostico de información"

	Grado de satisfacción E,B,R,D	Número de máquinas con esta aplicación.	Usado por el D.S.M.M.R.F.	usado por las coordinaciones	usado por el personal operativo
Procesador de palabras Nombre (s)	B	1	X	( )	( )
Hojas de cálculo / graficadores Nombre (s)	B	1	X	( )	( )
Lenguajes / manejadores de bases de datos Nombre (s)		—	X	( )	( )
Presentador textos Nombre (s)	B	SI	X	( )	( )
Correo electrónico / control de proyectos Nombre (s)		SI	X	( )	( )
Otros Nombre (s)					

Cuestionario de diagnóstico actual

"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

D) Hardware instalado "Diagnostico de información"

	Grado de Satisfacción E,B,R,D	Usado por el Depto	usado por las coordinaciones	usado por el personal operativo
Pc's No. de estación de trabajo Cantidad Modelo(s)	B	✓	( )	( )
Procesador Cantidad Marca (s)	—	✓	( )	( )
Uso de Impresora Cantidad Modelo(s)		✓	( )	( )
Red (Si/No) SI Tipo de Sistema Operativo: Windows NT (X) Windows 95 ( ) Windows 98 ( ) Windows 3.11. ( )		✓	( )	( )

F) Capacitación / Actualización "Diagnostico de información"

INDICACIONES Contestar sólo por los conductores de los trenes.	Excelente	Bueno	Regular	Deficiente
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	( )	( )	( )
Sistemas operativos de información Nombre (s) –Nivel Técnico.	( )	( )	( )	( )

G) Capacitación /Actualización "Diagnostico de información"

INDICACIONES: Contestar de acuerdo a la capacitación recibida.

	Excelente	Bueno	Regular	Deficiente
Procesador de palabras Nombre (s)	( )	( )	✓	( )
Hojas de cálculo / graficadores Nombre (s)	( )	( )	( )	✓
Lenguajes / manejadores de bases de datos Nombre (s)	( )	( )	( )	✓
Presentador / textos Nombre (s)	( )	( )	( )	✓
Correo electrónico / control de proyectos Nombre (s)	( )	( )	✓	( )

Nombre: OMAR CASTILLO M *Área:* DEPTO. SERV. M.M.R.F.

Cuestionario de diagnóstico actual

"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

Este cuestionario tiene la finalidad de conocer a grandes rasgos el estado en el que se encuentran los Sistemas y Equipos Informáticos utilizados para las diferentes actividades de las áreas del Taller.

A) Soluciones de Informática (.Diagnóstico de los Talleres La Paz).

Instrucciones: Marque con una cruz en los recuadros la respuesta que crea usted más conveniente de acuerdo a su criterio.

Servicios	Calificación en base al grado de satisfacción			
	Excelente	**Bueno**	**Regular**	**Deficiente**
• **Soluciones de consultoría** Asesoría. apoyo técnico y soporte presentado por el apoyo informático en la evaluación y solución de problemas presentados	( )	X	( )	( )
• **Soluciones de sistematización y capacitación en procesos** En la instalación de sistemas requeridos en el desarrollo de sus funciones operativas, tácticas y estratégicas	( )	( )	X	( )
• **Soluciones de desarrollo tecnológico** Evaluación y selección de tecnología de vanguardia:	( )	( )	X	( )
• **Servicios operativos** · Instalación de equipo de cómputo y telecomunicaciones · Capacitación en el uso de la tecnología · Atención a fallas de software y aplicaciones · Atención a fallas en equipos de cómputo y comunicaciones	( )	( )	( )	X

B) Sistemas de información instalados "diagnostico de informática"

INDICACIONES Contestar sólo por los conductores de los trenes.	Si	No
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	( )
Sistemas operativos de información Nombre (s) –Nivel Técnico.	( )	( )

C) Software instalado "Diagnostico de información"

	Grado de satisfacción E,B,R,D	Número de máquinas con esta aplicación.	Usado por el D.S.M.M.R.F	usado por las coordinaciones	usado por el personal operativo
Procesador de palabras Nombre (s) Word	R	1	( )	X	( )
Hojas de calculo / graficadores Nombre (s) Excel	B	1	( )	X	( )
Lenguajes - manejadores de bases de datos Nombre (s)			( )	( )	( )
Presentador - textos Nombre (s) Power Point	B	1	( )	X	( )
Correo electrónico - control de proyectos Nombre (s) Project Pert	B		( )	( )	( )
Otros Nombre (s)					

Cuestionario de diagnóstico actual
"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

D) Hardware instalado "Diagnostico de información"

	Grado de Satisfacción E,B,R,D	Usado por el Depto	usado por las coordinaciones	usado por el personal operativo
Pc's No. de estación de trabajo Cantidad Modelo(s)	B	⊠	( )	( )
Procesador Cantidad Marca (s)		⊠	( )	( )
Uso de Impresora Cantidad Modelo(s) HP LASERJET 5P	B	⊠	( )	( )
Red (Si/No) SI Tipo de Sistema Operativo: Windows NT ( ) Windows 95 ( ) Windows 98 (⊠) Windows 3.11. ( )	B	⊠	( )	( )

F) Capacitación / Actualización "Diagnostico de información"

INDICACIONES Contestar sólo por los conductores de los trenes.	Excelente	Bueno	Regular	Deficiente
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	( )	( )	( )
Sistemas operativos de información Nombre (s) –Nivel Técnico.	( )	( )	( )	( )

G) Capacitación /Actualización "Diagnostico de información"

INDICACIONES: Contestar de acuerdo a la capacitación recibida.

	Excelente	Bueno	Regular	Deficiente
Procesador de palabras Nombre (s) Word	( )	⊠	( )	( )
Hojas de cálculo / graficadores Nombre (s) Excel	( )	⊠	( )	( )
Lenguajes / manejadores de bases de datos Nombre (s)	( )	( )	( )	—
Presentador / textos Nombre (s) Power Point	( )	( )	⊠	( )
Correo electrónico / control de proyectos Nombre (s)	( )	( )	( )	—

114 *Nombre:* Rogelio Aguirre F *Área:* Mantto Mayor

Cuestionario de diagnóstico actual
"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

Este cuestionario tiene la finalidad de conocer a grandes rasgos el estado en el que se encuentran los Sistemas y Equipos Informáticos utilizados para las diferentes actividades de las áreas del Taller.

A) Soluciones de Informática (.Diagnóstico de los Talleres La Paz).

Instrucciones: Marque con una cruz en los recuadros la respuesta que crea usted más conveniente de acuerdo a su criterio.

Servicios	Calificación en base al grado de satisfacción			
	Excelente	Bueno	Regular	Deficiente
• **Soluciones de consultoría** Asesoría, apoyo técnico y soporte presentado por el apoyo informático en la evaluación y solución de problemas presentados	( )	( )	( )	(X)
• **Soluciones de sistematización y capacitación en procesos** En la instalación de sistemas requeridos en el desarrollo de sus funciones operativas, tácticas y estratégicas	( )	( )	X	( )
• **Soluciones de desarrollo tecnológico** Evaluación y selección de tecnología de vanguardia;	( )	( )	( )	X
• **Servicios operativos** · Instalación de equipo de cómputo y telecomunicaciones · Capacitación en el uso de la tecnología · Atención a fallas de software y aplicaciones · Atención a fallas en equipos de cómputo y comunicaciones	( )	( )	( )	X

B) Sistemas de información instalados "diagnostico de informática"

INDICACIONES Contestar sólo por los conductores de los trenes.	Si	No
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	( )
Sistemas operativos de información Nombre (s) –Nivel Técnico.	( )	( )

C) Software instalado "Diagnostico de información"

	Grado de satisfacción E,B,R,D	Número de máquinas con esta aplicación.	Usado por el D.S.M.M.R.F	usado por las coordinaciones	usado por el personal operativo
Procesador de palabras Nombre (s)	B		( )	( )	( )
Hojas de cálculo / graficadores Nombre (s)	B		( )	( )	( )
Lenguajes manejadores de bases de datos Nombre (s)			( )	( )	( )
Presentador textos Nombre (s)	B		( )	( )	( )
Correo electrónico / control de proyectos Nombre (s)			( )	( )	( )
Otros Nombre (s)					?

Cuestionario de diagnóstico actual

"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

D) Hardware instalado "Diagnostico de información"

	Grado de Satisfacción E,B,R,D	Usado por el Depto	usado por las coordinaciones	usado por el personal operativo
Pc´s No. de estación de trabajo Cantidad Modelo(s)	B	( )	( )	( )
Procesador Cantidad Marca (s)	—	( )	( )	( )
Uso de Impresora Cantidad Modelo(s)	B	( )	( )	( )
Red (Si/No) ____ Tipo de Sistema Operativo: Windows NT ( ) Windows 95 ( ) Windows 98 (✓) Windows 3.11. ( )	B	( )	( )	( )

F) Capacitación / Actualización "Diagnostico de información"

INDICACIONES Contestar sólo por los conductores de los trenes.	Excelente	Bueno	Regular	Deficiente
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	( )	( )	( )
Sistemas operativos de información Nombre (s) –Nivel Técnico.	( )	( )	( )	( )

G) Capacitación /Actualización "Diagnostico de información"

INDICACIONES: Contestar de acuerdo a la capacitación recibida.

	Excelente	Bueno	Regular	Deficiente
Procesador de palabras Nombre (s)	( )	✓	( )	( )
Hojas de cálculo / graficadores Nombre (s)	( )	✓	( )	( )
Lenguajes / manejadores de bases de datos Nombre (s)	( )	✓	( )	( )
Presentador / textos Nombre (s)	( )	✓	( )	( )
Correo electrónico / control de proyectos Nombre (s)	( )	( )	( )	( )

Nombre: _____ *Área:* _____

Cuestionario de diagnóstico actual

"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

Este cuestionario tiene la finalidad de conocer a grandes rasgos el estado en el que se encuentran los Sistemas y Equipos Informáticos utilizados para las diferentes actividades de las áreas del Taller.

A) Soluciones de Informática (.Diagnóstico de los Talleres La Paz).

Instrucciones: Marque con una cruz en los recuadros la respuesta que crea usted más conveniente de acuerdo a su criterio.

Servicios	Calificación en base al grado de satisfacción			
	Excelente	Bueno	Regular	Deficiente
• **Soluciones de consultoría** Asesoría, apoyo técnico y soporte presentado por el apoyo informático en la evaluación y solución de problemas presentados	( )	X	( )	( )
• **Soluciones de sistematización y capacitación en procesos** En la instalación de sistemas requeridos en el desarrollo de sus funciones operativas, tácticas y estratégicas	( )	X	( )	( )
• **Soluciones de desarrollo tecnológico** Evaluación y selección de tecnología de vanguardia;	( )	X	( )	( )
• **Servicios operativos** Instalación de equipo de cómputo y telecomunicaciones Capacitación en el uso de la tecnología Atención a fallas de software y aplicaciones Atención a fallas en equipos de cómputo y comunicaciones	( )	X	( )	( )

B) Sistemas de información instalados "diagnostico de informática"

INDICACIONES Contestar sólo por los conductores de los trenes.	Si	No
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	( )
Sistemas operativos de información Nombre (s) –Nivel Técnico. Agata Lotus y Agata Medio	X	( )

C) Software instalado "Diagnostico de información"

	Grado de satisfacción E,B,R,D	Número de máquinas con esta aplicación.	Usado por el D.S.M.M.R.F	usado por las coordinaciones	usado por el personal operativo
Procesador de palabras Nombre (s)	B	1	( )	X	( )
Hojas de cálculo - graficadores Nombre (s)	B	1	( )	X	( )
Lenguajes - manejadores de bases de datos Nombre (s)	B	1	( )	X	( )
Presentador - textos Nombre (s)	B	1	( )	X	( )
Correo electrónico / control de proyectos Nombre (s)	—		( )	( )	( )
Otros Nombre (s)					

Cuestionario de diagnóstico actual

"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

D) Hardware instalado "Diagnostico de información"

	Grado de Satisfacción E,B,R,D	Usado por el Depto	usado por las coordinaciones	usado por el personal operativo
Pc's No. de estación de trabajo Cantidad Modelo(s)		( )	✓	( )
Procesador Cantidad Marca (s)		( )	✓	( )
Uso de Impresora Cantidad Modelo(s) Epson 130MT		( )	✓	( )
Red (Si/No) Tipo de Sistema Operativo: Windows NT ( ) Windows 95 ( ) Windows 98 ( ) Windows 3.11. ( )		( )	✓	( )

F) Capacitación / Actualización "Diagnostico de información"

INDICACIONES Contestar sólo por los conductores de los trenes.	Excelente	Bueno	Regular	Deficiente
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	( )	✓	( )
Sistemas operativos de información Nombre (s) –Nivel Técnico.	( )	( )	✓	( )

G) Capacitación /Actualización "Diagnostico de información"

INDICACIONES: Contestar de acuerdo a la capacitación recibida.

	Excelente	Bueno	Regular	Deficiente
Procesador de palabras Nombre (s)	( )	✓	( )	( )
Hojas de cálculo / graficadores Nombre (s)	( )	✓	( )	( )
Lenguajes / manejadores de bases de datos Nombre (s)	( )	✓	( )	( )
Presentador / textos Nombre (s)	( )	✓	( )	( )
Correo electrónico / control de proyectos Nombre (s)	( )	( )	( )	( )

Nombre: Jaime Garcia López Área: Mando Medio

Cuestionario de diagnóstico actual

"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

Este cuestionario tiene la finalidad de conocer a grandes rasgos el estado en el que se encuentran los Sistemas y Equipos Informáticos utilizados para las diferentes actividades de las áreas del Taller.

A) Soluciones de Informática (.Diagnóstico de los Talleres La Paz).

Instrucciones: Marque con una cruz en los recuadros la respuesta que crea usted más conveniente de acuerdo a su criterio.

Servicios	Calificación en base al grado de satisfacción			
	Excelente	Bueno	Regular	Deficiente
• **Soluciones de consultoría** Asesoría, apoyo técnico y soporte presentado por el apoyo informático en la evaluación y solución de problemas presentados	( )	( )	(X)	( )
• **Soluciones de sistematización y capacitación en procesos** En la instalación de sistemas requeridos en el desarrollo de sus funciones operativas, tácticas y estratégicas	( )	( )	(X)	( )
• **Soluciones de desarrollo tecnológico** Evaluación y selección de tecnología de vanguardia;	( )	( )	( )	(X)
• **Servicios operativos** Instalación de equipo de cómputo y telecomunicaciones Capacitación en el uso de la tecnología Atención a fallas de software y aplicaciones Atención a fallas en equipos de cómputo y comunicaciones	( )	( )	(X)	( )

B) Sistemas de información instalados "diagnostico de informática"

INDICACIONES Contestar sólo por los conductores de los trenes.	Si	No
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	( )
Sistemas operativos de información Nombre (s) –Nivel Técnico.	( )	( )

C) Software instalado "Diagnostico de información"

	Grado de satisfacción E,B,R,D	Número de máquinas con esta aplicación.	Usado por el D.S.M.M.R.F.	usado por las coordinaciones	usado por el personal operativo
Procesador de palabras Nombre (s)	B		( )	(X)	( )
Hojas de cálculo / graficadores Nombre (s)	B		( )	(X)	( )
Lenguajes - manejadores de bases de datos Nombre (s)			( )	( )	( )
Presentador / textos Nombre (s)	B		( )	(X)	( )
Correo electrónico / control de proyectos Nombre (s)			( )	( )	( )
Otros Nombre (s)					

Cuestionario de diagnóstico actual
"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

D) Hardware instalado "Diagnostico de información"

	Grado de Satisfacción E,B,R,D	Usado por el Depto	usado por las coordinaciones	usado por el personal operativo
Pc's No. de estación de trabajo Cantidad Modelo(s)	B	( )	✓	( )
Procesador Cantidad Marca (s)	B	( )	✓	( )
Uso de Impresora Cantidad Modelo(s)	B	( )	✓	( )
Red (Si/No) Si. Tipo de Sistema Operativo: Windows NT ( ) Windows 95 ( ) Windows 98 ( ) Windows 3.11. ( )	B	( )	✓	( )

F) Capacitación / Actualización "Diagnostico de información"

INDICACIONES Contestar sólo por los conductores de los trenes.	Excelente	Bueno	Regular	Deficiente
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	( )	( )	( )
Sistemas operativos de información Nombre (s) –Nivel Técnico.	( )	( )	( )	( )

G) Capacitación /Actualización "Diagnostico de información"

INDICACIONES: Contestar de acuerdo a la capacitación recibida.

	Excelente	Bueno	Regular	Deficiente
Procesador de palabras Nombre (s)	( )	( )	( )	✓
Hojas de cálculo / graficadores Nombre (s)	( )	( )	( )	✓
Lenguajes / manejadores de bases de datos Nombre (s)	( )	( )	( )	✓
Presentador / textos Nombre (s)	( )	( )	( )	✓
Correo electrónico / control de proyectos Nombre (s)	( )	( )	( )	✓

120 *Nombre:* Ing Tomas Salinas Hartwig *Área:* Servicios Electricos.

Cuestionario de diagnóstico actual

"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

Este cuestionario tiene la finalidad de conocer a grandes rasgos el estado en el que se encuentran los Sistemas y Equipos Informáticos utilizados para las diferentes actividades de las áreas del Taller.

A) Soluciones de Informática (.Diagnóstico de los Talleres La Paz).

Instrucciones: Marque con una cruz en los recuadros la respuesta que crea usted más conveniente de acuerdo a su criterio.

Servicios	Calificación en base al grado de satisfacción			
	Excelente	Bueno	Regular	Deficiente
• **Soluciones de consultoría** Asesoría, apoyo técnico y soporte presentado por el apoyo informático en la evaluación y solución de problemas presentados	( )	(X)	( )	( )
• **Soluciones de sistematización y capacitación en procesos** En la instalación de sistemas requeridos en el desarrollo de sus funciones operativas, tácticas y estratégicas	( )	(X)	( )	( )
• **Soluciones de desarrollo tecnológico** Evaluación y selección de tecnología de vanguardia;	( )	( )	(X)	( )
• **Servicios operativos** Instalación de equipo de cómputo y telecomunicaciones Capacitación en el uso de la tecnología Atención a fallas de software y aplicaciones Atención a fallas en equipos de cómputo y comunicaciones	( )	(X)	( )	( )

B) Sistemas de información instalados "diagnostico de informática"

INDICACIONES Contestar sólo por los conductores de los trenes.	Si	No
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	(X)
Sistemas operativos de información Nombre (s) –Nivel Técnico.	( )	(X)

C) Software instalado "Diagnostico de información"

	Grado de satisfacción E,B,R,D	Número de máquinas con esta aplicación.	Usado por el D.S.M.M.R.F	usado por las coordinaciones	usado por el personal operativo
Procesador de palabras Nombre (s)	B	1	(X)	( )	( )
Hojas de cálculo / graficadores Nombre (s)	B	1	(X)	( )	( )
Lenguajes . manejadores de bases de datos Nombre (s)	B	4	(X)	( )	( )
Presentador / textos Nombre (s)	B	1	( )	(X)	( )
Correo electrónico / control de proyectos Nombre (s)	B		( )	( )	( )
Otros Nombre (s)					

Cuestionario de diagnóstico actual

"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

D) Hardware instalado "Diagnostico de información"

	Grado de Satisfacción E,B,R,D	Usado por el Depto	usado por las coordinaciones	usado por el personal operativo
Pc's No. de estación de trabajo Cantidad Modelo(s)	B	X	X	( )
Procesador Cantidad Marca (s)		( )	( )	( )
Uso de Impresora Cantidad Modelo(s)	B	X	X	( )
Red (Si/No) S Tipo de Sistema Operativo: Windows NT ( ) Windows 95 ( ) Windows 98 ( ) Windows 3.11. ( )	B	X	X	( )

F) Capacitación / Actualización "Diagnostico de información"

INDICACIONES Contestar sólo por los conductores de los trenes.	Excelente	Bueno	Regular	Deficiente
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	( )	( )	( )
Sistemas operativos de información Nombre (s) –Nivel Técnico.	( )	( )	( )	( )

G) Capacitación /Actualización "Diagnostico de información"

INDICACIONES: Contestar de acuerdo a la capacitación recibida.

	Excelente	Bueno	Regular	Deficiente
Procesador de palabras Nombre (s)	( )	( )	✓	( )
Hojas de cálculo / graficadores Nombre (s)	( )	( )	✓	( )
Lenguajes / manejadores de bases de datos Nombre (s)	( )	✓	( )	( )
Presentador / textos Nombre (s)	( )	( )	✓	( )
Correo electrónico / control de proyectos Nombre (s)	( )	( )	( )	✓

 Nombre: Mariano Romero Aguilar *Área:* Coordinación de Servicios.

Cuestionario de diagnóstico actual

"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

Este cuestionario tiene la finalidad de conocer a grandes rasgos el estado en el que se encuentran los Sistemas y Equipos Informáticos utilizados para las diferentes actividades de las áreas del Taller.

A) Soluciones de Informática (.Diagnóstico de los Talleres La Paz).

Instrucciones: Marque con una cruz en los recuadros la respuesta que crea usted más conveniente de acuerdo a su criterio.

Servicios	Calificación en base al grado de satisfacción			
	Excelente	Bueno	Regular	Deficiente
• **Soluciones de consultoría** Asesoría, apoyo técnico y soporte presentado por el apoyo informático en la evaluación y solución de problemas presentados	( )	( )	( )	(X)
• **Soluciones de sistematización y capacitación en procesos** En la instalación de sistemas requeridos en el desarrollo de sus funciones operativas, tácticas y estratégicas	( )	( )	( )	(X)
• **Soluciones de desarrollo tecnológico** Evaluación y selección de tecnología de vanguardia;	( )	( )	( )	(X)
• **Servicios operativos** · Instalación de equipo de cómputo y telecomunicaciones · Capacitación en el uso de la tecnología · Atención a fallas de software y aplicaciones · Atención a fallas en equipos de cómputo y comunicaciones	( )	( )	( )	(X)

B) Sistemas de información instalados "diagnostico de informática"

INDICACIONES Contestar sólo por los conductores de los trenes.	Si	No
Sistemas tacticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	( )
Sistemas operativos de información Nombre (s) –Nivel Tecnico.	( )	( )

C) Software instalado "Diagnostico de información"

	Grado de satisfacción E,B,R,D	Número de máquinas con esta aplicación.	Usado por el D.S.M.M.R.F	usado por las coordinaciones	usado por el personal operativo
Procesador de palabras Nombre (s)	R	1	( )	(X)	( )
Hojas de calculo / graficadores Nombre (s)	B	1	( )	(X)	( )
Lenguajes - manejadores de bases de datos Nombre (s)	B	1	( )	(X)	( )
Presentador / textos Nombre (s)	R	1	( )	(X)	( )
Correo electronico / control de proyectos Nombre (s)	—	NO	( )	( )	( )
Otros Nombre (s)					

Cuestionario de diagnóstico actual
"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

D) Hardware instalado "Diagnostico de información"

	Grado de Satisfacción E,B,R,D	Usado por el Depto	usado por las coordinaciones	usado por el personal operativo
Pc's No. de estación de trabajo Cantidad Modelo(s)	R	( )	⊗	( )
Procesador Cantidad Marca (s)	—	( )	( )	( )
Uso de Impresora Cantidad Modelo(s)		( )	⊗	( )
Red (Si/No) SI Tipo de Sistema Operativo: Windows NT ( ) Windows 95 ( ) Windows 98 (⊗) Windows 3.11. ( )	R	( )	⊗	( )

F) Capacitación / Actualización "Diagnostico de información"

INDICACIONES Contestar sólo por los conductores de los trenes.	Excelente	Bueno	Regular	Deficiente
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	( )	( )	( )
Sistemas operativos de información Nombre (s) –Nivel Técnico.	( )	⊗	( )	( )

G) Capacitación /Actualización "Diagnostico de información"

INDICACIONES: Contestar de acuerdo a la capacitación recibida.

	Excelente	Bueno	Regular	Deficiente
Procesador de palabras Nombre (s)	( )	⊗	( )	( )
Hojas de cálculo / graficadores Nombre (s)	( )	⊗	( )	( )
Lenguajes / manejadores de bases de datos Nombre (s)	( )	( )	⊗	( )
Presentador / textos Nombre (s)	( )	( )	( )	⊗
Correo electrónico / control de proyectos Nombre (s)	( )	( )	( )	⊗

Nombre: RICARDO RIQUELME PALACIOS *Área:* MANTTO. MAYOR

Cuestionario de diagnóstico actual

"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

Este cuestionario tiene la finalidad de conocer a grandes rasgos el estado en el que se encuentran los Sistemas y Equipos Informáticos utilizados para las diferentes actividades de las áreas del Taller.

A) Soluciones de Informática (.Diagnóstico de los Talleres La Paz).

Instrucciones: Marque con una cruz en los recuadros la respuesta que crea usted más conveniente de acuerdo a su criterio.

Servicios	Calificación en base al grado de satisfacción			
	Excelente	Bueno	Regular	Deficiente
• **Soluciones de consultoría** Asesoría, apoyo técnico y soporte presentado por el apoyo informático en la evaluación y solución de problemas presentados	( )	( )	( )	( )
• **Soluciones de sistematización y capacitación en procesos** En la instalación de sistemas requeridos en el desarrollo de sus funciones operativas, tácticas y estratégicas	( )	( )	( )	( )
• **Soluciones de desarrollo tecnológico** Evaluación y selección de tecnología de vanguardia;	( )	( )	( )	( )
• **Servicios operativos** Instalación de equipo de cómputo y telecomunicaciones Capacitación en el uso de la tecnología Atención a fallas de software y aplicaciones Atención a fallas en equipos de cómputo y comunicaciones	( )	( )	( )	( )

B) Sistemas de información instalados "diagnostico de informática".

INDICACIONES Contestar sólo por los conductores de los trenes.	Si	No
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	X	( )
Sistemas operativos de información Nombre (s) –Nivel Técnico. ACATE LINUX – ACATE MEDIA (SEÑALES DE TREN Y COMUNICACION A USUARIOS)	X	( )

C) Software instalado "Diagnostico de información"

	Grado de satisfacción E,B,R,D	Número de máquinas con esta aplicación.	Usado por el D.S.M.M.R.F	usado por las coordinaciones	usado por el personal operativo
Procesador de palabras Nombre (s)	B	1	( )	X	( )
Hojas de cálculo / graficadores Nombre (s)	B	1	( )	X	( )
Lenguajes / manejadores de bases de datos Nombre (s)	B	1	( )	X	( )
Presentador / textos Nombre (s)	B	1	( )	X	( )
Correo electrónico / control de proyectos Nombre (s)	D	1	( )	X	( )
Otros Nombre (s)					

Cuestionario de diagnóstico actual

"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

D) Hardware instalado "Diagnostico de información"

	Grado de Satisfacción E,B,R,D	Usado por el Depto	usado por las coordinaciones	usado por el personal operativo
Pc's No. de estación de trabajo Cantidad Modelo(s)	D	( )	(✓)	( )
Procesador Cantidad Marca (s)	R	( )	(✓)	( )
Uso de Impresora Cantidad Modelo(s) H.P. LaserJet 5Si	B	( )	(✓)	( )
Red (Si/No) Si Tipo de Sistema Operativo: Windows NT ( ) Windows 95 ( ) Windows 98 (✓) Windows 3.11. ( )	B	( )	(✓)	( )

F) Capacitación / Actualización "Diagnostico de información"

INDICACIONES Contestar sólo por los conductores de los trenes.	Excelente	Bueno	Regular	Deficiente
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	( )	(✓)	( )
Sistemas operativos de información Nombre (s) –Nivel Técnico.	( )	(✓)	( )	( )

G) Capacitación /Actualización "Diagnostico de información"

INDICACIONES: Contestar de acuerdo a la capacitación recibida.

	Excelente	Bueno	Regular	Deficiente
Procesador de palabras Nombre (s)	( )	( )	( )	(✓)
Hojas de cálculo / graficadores Nombre (s)	( )	( )	( )	(✓)
Lenguajes / manejadores de bases de datos Nombre (s)	( )	( )	(✓)	( )
Presentador / textos Nombre (s)	( )	( )	( )	(✓)
Correo electrónico / control de proyectos Nombre (s)	( )	( )	( )	(✓)

Nombre: EZEQUIEL A. COZORES M. *Área:* INGENIERIA MAT. ROD. F.

Cuestionario de diagnóstico actual

"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

Este cuestionario tiene la finalidad de conocer a grandes rasgos el estado en el que se encuentran los Sistemas y Equipos Informáticos utilizados para las diferentes actividades de las áreas del Taller.

A) Soluciones de Informática (.Diagnóstico de los Talleres La Paz).

Instrucciones: Marque con una cruz en los recuadros la respuesta que crea usted más conveniente de acuerdo a su criterio.

Servicios	Calificación en base al grado de satisfacción			
	Excelente	Bueno	Regular	Deficiente
• **Soluciones de consultoría** Asesoría, apoyo técnico y soporte presentado por el apoyo informático en la evaluación y solución de problemas presentados	( )	✓	( )	( )
• **Soluciones de sistematización y capacitación en procesos** En la instalación de sistemas requeridos en el desarrollo de sus funciones operativas, tácticas y estratégicas	( )	( )	✓	( )
• **Soluciones de desarrollo tecnológico** Evaluación y selección de tecnología de vanguardia;	( )	( )	✓	( )
• **Servicios operativos** · Instalación de equipo de cómputo y telecomunicaciones · Capacitación en el uso de la tecnología · Atención a fallas de software y aplicaciones · Atención a fallas en equipos de cómputo y comunicaciones	( )	✓	( )	( )

B) Sistemas de información instalados "diagnostico de informática"

INDICACIONES Contestar sólo por los conductores de los trenes.	Si	No
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	( )
Sistemas operativos de información Nombre (s) –Nivel Técnico.	( )	( )

C) Software instalado "Diagnostico de información"

	Grado de satisfacción E,B,R,D	Número de máquinas con esta aplicación.	Usado por el D.S.M.M.R.F	usado por las coordinaciones	usado por el personal operativo
Procesador de palabras Nombre (s)	B	1	( )	(X)	( )
Hojas de cálculo / graficadores Nombre (s)	B	1	( )	(X)	( )
Lenguajes / manejadores de bases de datos Nombre (s)	B	1	( )	( )	( )
Presentador / textos Nombre (s)	B		( )	(X	( )
Correo electrónico / control de proyectos Nombre (s)	—		( )	( )	( )
Otros Nombre (s)	—				

Cuestionario de diagnóstico actual
"Etapa preliminar de Seguridad Informática de los Talleres la Paz del Sistema de Transporte Colectivo Metro"

D) Hardware instalado "Diagnostico de información"

	Grado de Satisfacción E,B,R,D	Usado por el Depto	usado por las coordinaciones	usado por el personal operativo
Pc's No. de estación de trabajo Cantidad Modelo(s)	B	( )	✓	( )
Procesador Cantidad Marca (s)		( )	( )	( )
Uso de Impresora Cantidad Modelo(s)	B	( )	✓	( )
Red (Si/No) Si Tipo de Sistema Operativo: Windows NT ( ) Windows 95 ( ) Windows 98 (X) Windows 3.11. ( )	B	( )	✓	( )

F) Capacitación / Actualización "Diagnostico de información"

INDICACIONES Contestar sólo por los conductores de los trenes.	Excelente	Bueno	Regular	Deficiente
Sistemas tácticos de información (aplicación en trenes) Nombre (s) –Mandos Intermedios.	( )	( )	( )	( )
Sistemas operativos de información Nombre (s) –Nivel Técnico.	( )	( )	( )	( )

G) Capacitación /Actualización "Diagnostico de información"

INDICACIONES: Contestar de acuerdo a la capacitación recibida.

	Excelente	Bueno	Regular	Deficiente
Procesador de palabras Nombre (s)	( )	( )	✓	( )
Hojas de cálculo / graficadores Nombre (s)	( )	( )	✓	( )
Lenguajes / manejadores de bases de datos Nombre (s)	( )	( )	( )	✓
Presentador / textos Nombre (s)	( )	( )	( )	✓
Correo electrónico / control de proyectos Nombre (s)	( )	( )	( )	✓

Nombre: ING ANTONIO PEREZ ROMERO *Área:* MANTTO ELECTROMECANICO

ANEXO 3

Cuestionarios de Seguridad

Analisis del Cuestionario sobre Seguridad Física

8 cuestionarios aplicados

A) Ubicación y construcción de las instalaciones

PREGUNTA 1

El Edificio cuenta con salidas de escape en caso de emergencia?

RESPUESTAS:

SI	No
2	6

PREGUNTA 2

Existen ventanas grandes que permitan la entrada del sol directamente en los equipos?

RESPUESTAS:

SI	No
2	6

B) Aire acondicionado

PREGUNTA 3

Los ductos de aire se encuentran libres de polvo?

RESPUESTAS

SI	No
1	4

C) Instalación Electrica y suministro de energía?

PREGUNTA 4

Se cuenta con tierra física?

RESPUESTAS

SI	No
6	2

PREGUNTA 5

Los cables se encuentran debidamente identificados (positivo, negativo, tierra física)?

RESPUESTAS

SI	No
4	4

PREGUNTA 6

Los contactos del equipo de cómputo están debidamente identificados?

RESPUESTAS

SI	No
5	3

PREGUNTA 7

Se tiene conectado a los contactos del equipo con otro equipo electronico?

RESPUESTAS

SI	No
2	6

PREGUNTA 8

Se tienen reguladores para los equipos de cómputo?

RESPUESTAS

SI	No
6	2

PREGUNTA 9

Se tiene equipo No-break?

RESPUESTAS

SI	No
1	7

PREGUNTA 10

Aproximadamente cuanto es el tiempo que se da para respaldar los archivos o para continuar el proceso?

RESPUESTAS

a) 15 minutos	
b) 30 minutos	1
c) 1 hora	1

PREGUNTA 11

Los cables están dentro de los paneles y canales eléctricos?

RESPUESTAS

SI	No
4	4

Analisis del Cuestionario sobre Seguridad Física

D) Autorización de Acceso

PREGUNTA 12

Existe personal de vigilancia en la institución?

RESPUESTAS

Si	No
8	

PREGUNTA 13

Se identifica a la persona que ingresa?

RESPUESTAS

Si	No
8	

E) Extintores

PREGUNTA 14

Existen extintores de fuego?

RESPUESTAS

a) Manuales 7
b) Automático
c) No existen 1

PREGUNTA 15

Se ha capacitado al personal en el manejo de estos?

RESPUESTAS

Si	No
6	2

PREGUNTA 16

Los extintores funcionan a base de ?

RESPUESTAS

a) Agua 1
b) Gas 3
c) Otros POLVO QUIMICO
ABC
FOSFATO MONOAMONICO
CO2

PREGUNTA 17

Se han tomado medidas para minimizar la posibilidad de fuego?

RESPUESTAS

a) Evitando artículos inflamables 4
b) Prohibiendo fumar 2
c) No se ha previsto 2

"CUESTIONARIO DE SEGURIDAD FÍSICA"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Ubicación y construcción de las instalaciones.

1. ¿El edificio cuenta con salidas de escape en caso de emergencia?
   Si ( ) No (✓)
2. ¿Existen ventanas grandes que permitan la entrada del sol directamente en los equipos?
   Si ( ) No (✓)

B) Aire acondicionado.

3. ¿Los ductos de aire se encuentran libres de polvo?
   Si ( ) No (✓)

C) Instalación eléctrica y suministro de energía.

4. ¿Se cuenta con tierra física?
   Si (✓) No ( )
5. ¿Los cables se encuentran debidamente identificados (positivo, negativo, tierra física)?
   Si ( ) No (✓)
6. ¿Los contactos del equipo de cómputo están debidamente identificados?
   Si (✓) No ( )
7. ¿Se tiene conectado a los contactos de equipo de cómputo con otro equipo electrónico?
   Si ( ) No (✓)
8. ¿Se tienen reguladores para los equipos de cómputo?
   Si (✓) No ( )
9. ¿Se tiene equipo No-break'?
   Si (✓) No ( )
10. ¿Aproximadamente cuánto es el tiempo que se da para respaldar los archivos o para continuar el proceso?
    a) 15 minutos ( ) b) 30 minutos (✓) c) 1 hora ( )
11. ¿Los cables están dentro de los paneles y canales eléctricos?
    Si ( ) No (✓)

D) Autorización de accesos.

12. ¿Existe personal de vigilancia en la institución?
    Si (✓) No ( )
13. ¿Se identifica a la persona que ingresa?
    Si (✓) No ( )

E) Extintores.

14. ¿Existen extintores de fuego?
    a) Manuales (✓) b) Automáticos ( ) c) No existen ( )
15. ¿Se ha capacitado al personal en el manejo de éstos?
    Si (✓) No ( )
16. ¿Los extintores funcionan a base de?
    a) Agua ( ) b) Gas ( ) Otros (menciónelos). Polvo Químico
17. ¿Se han tomado medidas para minimizar la posibilidad de fuego?
    a) Evitando artículo inflamables ( )
    b) Prohibiendo fumar en las áreas de riesgo ( )
    c) No se ha previsto. (✓)

"CUESTIONARIO DE SEGURIDAD FÍSICA"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Ubicación y construcción de las instalaciones.

1. ¿El edificio cuenta con salidas de escape en caso de emergencia?
   Si ( ) No (X)
2. ¿Existen ventanas grandes que permitan la entrada del sol directamente en los equipos?
   Si ( ) No (X)

B) Aire acondicionado.

3. ¿Los ductos de aire se encuentran libres de polvo?
   Si ( ) No ( )

C) Instalación eléctrica y suministro de energía.

4. ¿Se cuenta con tierra física?
   Si (X) No ( )
5. ¿Los cables se encuentran debidamente identificados (positivo, negativo, tierra física)?
   Si (X) No ( )
6. ¿Los contactos del equipo de cómputo están debidamente identificados?
   Si (X) No ( )
7. ¿Se tiene conectado a los contactos de equipo de cómputo con otro equipo electrónico?
   Si ( ) No (X)
8. ¿Se tienen reguladores para los equipos de cómputo?
   Si ( ) No (X)
9. ¿Se tiene equipo No-break?
   Si ( ) No (X)
10. ¿Aproximadamente cuánto es el tiempo que se da para respaldar los archivos o para continuar el proceso?
    a) 15 minutos ( ) b) 30 minutos ( ) c) 1 hora (X) .
11. ¿Los cables están dentro de los paneles y canales eléctricos?
    Si (X) No ( )

D) Autorización de accesos.

12. ¿Existe personal de vigilancia en la institución?
    Si (X) No ( )
13. ¿Se identifica a la persona que ingresa?
    Si (X) No ( )

E) Extintores.

14. ¿Existen extintores de fuego?
    a) Manuales (X) b) Automáticos ( ) c) No existen ( )
15. ¿Se ha capacitado al personal en el manejo de éstos?
    Si (X) No ( )
16. ¿Los extintores funcionan a base de?
    a) Agua (Y) b) Gas (X) Otros (menciónelos)_____
17. ¿Se han tomado medidas para minimizar la posibilidad de fuego?
    a) Evitando artículo inflamables (X)
    b) Prohibiendo fumar en las áreas de riesgo ( )
    c) No se ha previsto ( )

"CUESTIONARIO DE SEGURIDAD FÍSICA"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Ubicación y construcción de las instalaciones.

1. ¿El edificio cuenta con salidas de escape en caso de emergencia?
   Si ( ) No (✓)
2. ¿Existen ventanas grandes que permitan la entrada del sol directamente en los equipos?
   Si (✓) No ( )

B) Aire acondicionado.

3. ¿Los ductos de aire se encuentran libres de polvo?
   Si ( ) No (✓)

C) Instalación eléctrica y suministro de energía.

4. ¿Se cuenta con tierra física?
   Si ( ) No (✓)
5. ¿Los cables se encuentran debidamente identificados (positivo, negativo, tierra física)?
   Si ( ) No ( )
6. ¿Los contactos del equipo de cómputo están debidamente identificados?
   Si ( ) No (✓)
7. ¿Se tiene conectado a los contactos de equipo de cómputo con otro equipo electrónico?
   Si ( ) No (✓)
8. ¿Se tienen reguladores para los equipos de cómputo?
   Si (✓) No ( )
9. ¿Se tiene equipo No-break?
   Si ( ) No (✓)
10. ¿Aproximadamente cuánto es el tiempo que se da para respaldar los archivos o para continuar el proceso?
    a) 15 minutos ( ) b) 30 minutos ( ) c) 1 hora ( )
11. ¿Los cables están dentro de los paneles y canales eléctricos?
    Si ( ) No (✓)

D) Autorización de accesos.

12. ¿Existe personal de vigilancia en la institución?
    Si (✓) No ( )
13. ¿Se identifica a la persona que ingresa?
    Si (✓) No ( )

E) Extintores.

14. ¿Existen extintores de fuego?
    a) Manuales (✓) b) Automáticos ( ) c) No existen ( )
15. ¿Se ha capacitado al personal en el manejo de éstos?
    Si ( ) No (✓)
16. ¿Los extintores funcionan a base de?
    a) Agua ( ) b) Gas (✓) Otros (mencionelos)_____
17. ¿Se han tomado medidas para minimizar la posibilidad de fuego?
    a) Evitando artículo inflamables (✓)
    b) Prohibiendo fumar en las areas de riesgo ( )
    c) No se ha previsto ( )

"CUESTIONARIO DE SEGURIDAD FÍSICA"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Ubicación y construcción de las instalaciones.

1. ¿El edificio cuenta con salidas de escape en caso de emergencia?
   Si ( ) No (X)
2. ¿Existen ventanas grandes que permitan la entrada del sol directamente en los equipos?
   Si ( ) No (X)

B) Aire acondicionado.

3. ¿Los ductos de aire se encuentran libres de polvo?
   Si ( ) No ( )

C) Instalación eléctrica y suministro de energía.

4. ¿Se cuenta con tierra física?
   Si ( ) No ( )
5. ¿Los cables se encuentran debidamente identificados (positivo, negativo, tierra física)?
   Si ( ) No (X)
6. ¿Los contactos del equipo de cómputo están debidamente identificados?
   Si ( ) No ( )
7. ¿Se tiene conectado a los contactos de equipo de cómputo con otro equipo electrónico?
   Si (X) No ( )
8. ¿Se tienen reguladores para los equipos de cómputo?
   Si ( ) No (X)
9. ¿Se tiene equipo No-break?
   Si ( ) No (X)
10. ¿Aproximadamente cuánto es el tiempo que se da para respaldar los archivos o para continuar el proceso?
    a) 15 minutos ( ) b) 30 minutos ( ) c) 1 hora (X)
11. ¿Los cables están dentro de los paneles y canales eléctricos?
    Si (X) No ( )

D) Autorización de accesos.

12. ¿Existe personal de vigilancia en la institución?
    Si (X) No ( )
13. ¿Se identifica a la persona que ingresa?
    Si (X) No ( )

E) Extintores.

14. ¿Existen extintores de fuego?
    a) Manuales (X) b) Automáticos ( ) c) No existen ( )
15. ¿Se ha capacitado al personal en el manejo de éstos?
    Si ( ) No (X)
16. ¿Los extintores funcionan a base de?
    a) Agua ( ) b) Gas (X) Otros (menciónelos)_____
17. ¿Se han tomado medidas para minimizar la posibilidad de fuego?
    a) Evitando artículo inflamables (X)
    b) Prohibiendo fumar en las áreas de riesgo (X)
    c) No se ha previsto ( )

"CUESTIONARIO DE SEGURIDAD FÍSICA"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Ubicación y construcción de las instalaciones.

1. ¿El edificio cuenta con salidas de escape en caso de emergencia?
   Si ( ) No (✓)
2. ¿Existen ventanas grandes que permitan la entrada del sol directamente en los equipos?
   Si (✓) No ( )

B) Aire acondicionado.

3. ¿Los ductos de aire se encuentran libres de polvo?
   Si ( ) No ( )

C) Instalación eléctrica y suministro de energía.

4. ¿Se cuenta con tierra física?
   Si (✓) No ( )
5. ¿Los cables se encuentran debidamente identificados (positivo, negativo, tierra física)?
   Si ( ) No (✓)
6. ¿Los contactos del equipo de cómputo están debidamente identificados?
   Si ( ) No (✓)
7. ¿Se tiene conectado a los contactos de equipo de cómputo con otro equipo electrónico?
   Si (✓) No ( )
8. ¿Se tienen reguladores para los equipos de cómputo?
   Si (✓) No ( )
9. ¿Se tiene equipo No-break?
   Si ( ) No (✓)
10. ¿Aproximadamente cuánto es el tiempo que se da para respaldar los archivos o para continuar el proceso?
    a) 15 minutos ( ) b) 30 minutos ( ) c) 1 hora ( )
11. ¿Los cables están dentro de los paneles y canales eléctricos?
    Si (✓) No ( )

D) Autorización de accesos.

12. ¿Existe personal de vigilancia en la institución?
    Si (✓) No ( )
13. ¿Se identifica a la persona que ingresa?
    Si (✓) No ( )

E) Extintores.

14. ¿Existen extintores de fuego?
    a) Manuales (✓) b) Automáticos ( ) c) No existen ( )
15. ¿Se ha capacitado al personal en el manejo de éstos?
    Si (✓) No ( )
16. ¿Los extintores funcionan a base de?
    a) Agua ( ) b) Gas ( ) Otros (menciónelos) POLVO QUIMICO SECO ABC (CO2) BICARBONATO MONOFILO
17. ¿Se han tomado medidas para minimizar la posibilidad de fuego?
    a) Evitando artículo inflamables (✓)
    b) Prohibiendo fumar en las áreas de riesgo (✓)
    c) No se ha previsto ( )

"CUESTIONARIO DE SEGURIDAD FÍSICA"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Ubicación y construcción de las instalaciones.

1. ¿El edificio cuenta con salidas de escape en caso de emergencia?
   Si (X) No ( )
2. ¿Existen ventanas grandes que permitan la entrada del sol directamente en los equipos?
   Si ( ) No (X)

B) Aire acondicionado.

3. ¿Los ductos de aire se encuentran libres de polvo?
   Si (X) No ( )

C) Instalación eléctrica y suministro de energía.

4. ¿Se cuenta con tierra física?
   Si (X) No ( )
5. ¿Los cables se encuentran debidamente identificados (positivo, negativo, tierra física)?
   Si (X) No ( )
6. ¿Los contactos del equipo de cómputo están debidamente identificados?
   Si (X) No ( )
7. ¿Se tiene conectado a los contactos de equipo de cómputo con otro equipo electrónico?
   Si ( ) No (X)
8. ¿Se tienen reguladores para los equipos de cómputo?
   Si (X) No ( )
9. ¿Se tiene equipo No-break?
   Si ( ) No (X)
10. ¿Aproximadamente cuanto es el tiempo que se da para respaldar los archivos o para continuar el proceso?
    a) 15 minutos ( ) b) 30 minutos ( ) c) 1 hora ( )
11. ¿Los cables están dentro de los paneles y canales eléctricos?
    Si (X) No ( )

D) Autorización de accesos.

12. ¿Existe personal de vigilancia en la institución?
    Si (X) No ( )
13. ¿Se identifica a la persona que ingresa?
    Si (X) No ( )

E) Extintores.

14. ¿Existen extintores de fuego?
    a) Manuales (X) b) Automáticos ( ) c) No existen ( )
15. ¿Se ha capacitado al personal en el manejo de éstos?
    Si (X) No ( )
16. ¿Los extintores funcionan a base de?
    a) Agua ( ) b) Gas ( ) Otros (menciónelos) Polvo Quimico
17. ¿Se han tomado medidas para minimizar la posibilidad de fuego?
    a) Evitando artículo inflamables ( )
    b) Prohibiendo fumar en las áreas de riesgo (X)
    c) No se ha previsto ( )

"CUESTIONARIO DE SEGURIDAD FÍSICA"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Ubicación y construcción de las instalaciones.

1. ¿El edificio cuenta con salidas de escape en caso de emergencia?
   Si (✓) No ( )
2. ¿Existen ventanas grandes que permitan la entrada del sol directamente en los equipos?
   Si ( ) No (✓)

B) Aire acondicionado.

3. ¿Los ductos de aire se encuentran libres de polvo?
   Si ( ) No (✓)

C) Instalación eléctrica y suministro de energía.

4. ¿Se cuenta con tierra física?
   Si (✓) No ( )
5. ¿Los cables se encuentran debidamente identificados (positivo, negativo, tierra física)?
   Si (✓) No ( )
6. ¿Los contactos del equipo de cómputo están debidamente identificados?
   Si (✓) No ( )
7. ¿Se tiene conectado a los contactos de equipo de cómputo con otro equipo electrónico?
   Si ( ) No (✓)
8. ¿Se tienen reguladores para los equipos de cómputo?
   Si (✓) No ( )
9. ¿Se tiene equipo No-break?
   Si ( ) No (✓)
10. ¿Aproximadamente cuánto es el tiempo que se da para respaldar los archivos o para continuar el proceso?
    a) 15 minutos ( ) b) 30 minutos ( ) c) 1 hora ( )
11. ¿Los cables están dentro de los paneles y canales eléctricos?
    Si ( ) No (✓)

D) Autorización de accesos.

12. ¿Existe personal de vigilancia en la institución?
    Si (✓) No ( )
13. ¿Se identifica a la persona que ingresa?
    Si (✓) No ( )

E) Extintores.

14. ¿Existen extintores de fuego?
    a) Manuales ( ) b) Automáticos ( ) c) No existen (✓)
15. ¿Se ha capacitado al personal en el manejo de éstos?
    Si (✓) No ( )
16. ¿Los extintores funcionan a base de?
    a) Agua ( ) b) Gas ( ) Otros (menciónelos) CO_2
17. ¿Se han tomado medidas para minimizar la posibilidad de fuego?
    a) Evitando artículo inflamables (✓)
    b) Prohibiendo fumar en las áreas de riesgo ( )
    c) No se ha previsto ( )

"CUESTIONARIO DE SEGURIDAD FÍSICA"

Instrucciones: *Marque dentro de los paréntesis la respuesta que usted considere más conveniente de acuerdo a su experiencia (únicamente una sola respuesta).*

A) Ubicación y construcción de las instalaciones.

1. ¿El edificio cuenta con salidas de escape en caso de emergencia?
   Si ( ) No (✓)
2. ¿Existen ventanas grandes que permitan la entrada del sol directamente en los equipos?
   Si ( ) No (✓)

B) Aire acondicionado.

3. ¿Los ductos de aire se encuentran libres de polvo?
   Si ( ) No ( )

C) Instalación eléctrica y suministro de energía.

4. ¿Se cuenta con tierra física?
   Si ( ) No (✓)
5. ¿Los cables se encuentran debidamente identificados (positivo, negativo, tierra física)? Si (✓) No ( )
6. ¿Los contactos del equipo de cómputo están debidamente identificados?
   Si (✓) No ( )
7. ¿Se tiene conectado a los contactos de equipo de cómputo con otro equipo electrónico? Si ( ) No (✓)
8. ¿Se tienen reguladores para los equipos de cómputo?
   Si (✓) No ( )
9. ¿Se tiene equipo No-break?
   Si ( ) No (✓)
10. ¿Aproximadamente cuánto es el tiempo que se da para respaldar los archivos o para continuar el proceso?
    a) 15 minutos ( ) b) 30 minutos ( ) c) 1 hora ( )
11. ¿Los cables están dentro de los paneles y canales eléctricos?
    Si ( ) No (✓)

D) Autorización de accesos.

12. ¿Existe personal de vigilancia en la institución?
    Si (✓) No ( )
13. ¿Se identifica a la persona que ingresa?
    Si (✓) No ( )

E) Extintores.

14. ¿Existen extintores de fuego?
    a) Manuales (✓) b) Automáticos ( ) c) No existen ( )
15. ¿Se ha capacitado al personal en el manejo de éstos?
    Si (✓) No ( )
16. ¿Los extintores funcionan a base de?
    a) Agua ( ) b) Gas ( ) Otros (menciónelos) Polvos
17. ¿Se han tomado medidas para minimizar la posibilidad de fuego?
    a) Evitando artículo inflamables ( )
    b) Prohibiendo fumar (✓)

8.cuestionarios aplicados

A) Controles y procedimientos utilizados

PREGUNTA 1

Se cuenta con controles y procedimientos necesarios para garantizar la seguridad mínima requerida?

RESPUESTAS:

		Si	No
a) Procedimiento de llenado de dcumentos	a)	2	5
b) Procedimiento de encendido y apagado de la computadora	b)	3	5
c) Reinicialcion del equipo en caso de fallas	c)	2	5

PREGUNTA 2

Se cuenta con procedimientos para asegurar que los cambios en aplicaciones se documenten (indique el orden

RESPUESTAS:

		Si	No
a) Se encuentran justificados por medio de requerimientos de los usuarios	a)	2	5
b) Se encuentran descritos mencionando el objetivo y funcion de estos	b)	2	6
c) Se encuentran probados antes de ser implantados formalmente	c)	2	5
d) Se tienen en existencia manuales de referencia para el usuario	d)	1	6

B) Procesamiento de la Información

PREGUNTA 3

Se asegura que sólo los responsables de modificar los programas tengan acceso a éstos, explique de que forma?

RESPUESTAS:

Si	No
4	3

EXPLICACIONES:

De forma Verbal
Por medio de una clave de acceso
Informacion restringida
Acceso libre. ya que la información no es confidencial

PREGUNTA 4

Quien se encarga de efectuar las siguientes modificaciones a programas y aplicaciones?

RESPUESTAS:

	Actualizaciones	Eliminaciones	Consulta	Captura
Los mismos usuarios	5	3	5	6
El encargado (a) de brindar apoyo informatico	4	5	5	5
Programadores	0	0	0	0
Otros	0	0	0	2

PREGUNTA 5

Quién es el encargado de dar asistencia para la solución de problemas y aplicaciones que usted utiliza?

RESPUESTAS:

	a)	b)
a) La encargada de apoyo informático	7	3
b) Usted mismo		

PREGUNTA 6

Cuál es el estado que alcanza el o los problemas suscitados en las aplicaciones que utiliza?

RESPUESTAS:

	a)	b)
a) Resuelto, usted esta trabajando de nuevo pero el problema aún sigue latente	5	3
b) Cerrado se han realizado cambios para que ningun otro usuario tenga el mismo problema		

C) Seguridad en archivos

PREGUNTA 7

Se cuenta con procedimientos de respaldo de programas fuente, documentación y archivos en operación, mencionelos?

RESPUESTAS:

Si	No
2	5

Procedimientos:
Discos magneticos y de forma impresa

PREGUNTA 8

Se encuentra en un lugar distante el almacenamiento de colas de archivos?

RESPUESTAS:

Si	No
	6

PREGUNTA 9

Existen bitacoras para tener un control escrito de las modificaciones hechas a programas y aplicaciones?

RESPUESTAS:

Si	No
2	6

"CUESTIONARIO DE ADMINISTRACIÓN DE CAMBIOS Y PROBLEMAS EN APLICACIONES"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Controles y procedimientos utilizados.

1. Se cuenta con controles y procedimientos necesarios para garantizar la seguridad mínima requerida?

	Si	*No*
a) Procedimiento de llenado de documentos.	( )	(X)
b) Procedimiento de encendido y apagado de la computadora.	( )	(X)
c) Reinicialización del equipo en caso de fallas.	( )	(X)

2. ¿Se cuentan con procedimientos para asegurar que los cambios en aplicaciones se documenten?

	Si	*No*
a) Se encuentran justificados por medio de requerimientos de los usuarios.	( )	(X)
b) Se encuentran descritos mencionando el objetivo y función de éstos.	( )	(X)
c) Se encuentran probados antes de ser implantados formalmente.	(X)	( )
d) Se tienen en existencia manuales de referencia para el usuario.	( )	(X)

B) Procesamiento de la información.

3. ¿Se asegura que sólo los responsables de modificar los programas tengan acceso a éstos, explique de que forma?

Si (X) No ( )

por medio de claves de acceso

4. ¿Quien se encarga de efectuar las siguientes modificaciones a programas y aplicaciones?

	Actualización	Eliminación	Consulta	Captura
Los mismos usuarios	(X)	( )	(X)	(X)
El encargado (a) de brindar apoyo informatico	(X)	(X)	(X)	(X)
Programadores	( )	( )	( )	( )
Otros	( )	( )	( )	(X)

5. ¿Quién es el encargado de dar asistencia para la soluciones de problemas y aplicaciones que usted utiliza?

a) La encargada de apoyo informático. (X)
b) Usted mismo. (X)

6. ¿Cuál es el estado que alcanza el o los problemas suscitados en las aplicaciones que utiliza?

a) Resuelto, usted esta trabajando de nuevo, pero el problema aún sigue latente. (X)
b) Cerrado se han realizado cambios para que ningún otro usuario tenga el mismo problema. ( )

C) Seguridad en archivos.

7. Se cuenta con procedimientos de respaldo de programas fuente, documentación y archivos en operación, mencionelos?

Si ( ) No (X)

8. ¿Se encuentra en un lugar distante el almacenamiento de copias de los archivos?

Si (X) No ( )

9. ¿Existen bitacoras para tener un control por escrito de las modificaciones hechas a programas y aplicaciones?

Si (X) No ( )

"CUESTIONARIO DE ADMINISTRACIÓN DE CAMBIOS Y PROBLEMAS EN APLICACIONES"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Controles y procedimientos utilizados.

1. Se cuenta con controles y procedimientos necesarios para garantizar la seguridad mínima requerida?

	Si	*No*
a) Procedimiento de llenado de documentos.	( )	(X)
b) Procedimiento de encendido y apagado de la computadora.	( )	(X)
c) Reinicialización del equipo en caso de fallas.	( )	(X)

2. ¿Se cuentan con procedimientos para asegurar que los cambios en aplicaciones se documenten?

	Si	*No*
a) Se encuentran justificados por medio de requerimientos de los usuarios.	( )	(X)
b) Se encuentran descritos mencionando el objetivo y función de éstos.	( )	(X)
c) Se encuentran probados antes de ser implantados formalmente.	( )	(X)
d) Se tienen en existencia manuales de referencia para el usuario.	( )	(X)

B) Procesamiento de la información.

3. ¿Se asegura que sólo los responsables de modificar los programas tengan acceso a éstos, explique de que forma?

Si (X) No ( )

Unicamente de forma verbal

4. ¿Quién se encarga de efectuar las siguientes modificaciones a programas y aplicaciones?

	Actualización	Eliminación	Consulta	Captura
Los mismos usuarios	(X)	( )	(X)	(X)
El encargado (a) de brindar apoyo informático	(X)	(X)	(X)	(X)
Programadores	No Existen	( )	( )	( )
Otros	( )	( )	( )	(X)

5. ¿Quién es el encargado de dar asistencia para la soluciones de problemas y aplicaciones que usted utiliza?

a) La encargada de apoyo informático. (X)
b) Usted mismo. (X)

6. ¿Cuál es el estado que alcanza el o los problemas suscitados en las aplicaciones que utiliza?
a) Resuelto, usted esta trabajando de nuevo, pero el problema aún sigue latente. (X)
b) Cerrado se han realizado cambios para que ningún otro usuario tenga el mismo problema. ( )

C) Seguridad en archivos.

7. ¿Se cuenta con procedimientos de respaldo de programas fuente, documentación y archivos en operación mencionelos?

Si ( ) No (X)

8. ¿Se encuentra en un lugar distanto el almacenamiento de copias de los archivos?

Si ( ) No (X)

9. ¿Existen bitácoras para tener un control por escrito de las modificaciones hechas a programas y aplicaciones?

Si ( ) No (X)

"CUESTIONARIO DE ADMINISTRACIÓN DE CAMBIOS Y PROBLEMAS EN APLICACIONES"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Controles y procedimientos utilizados.

1. Se cuenta con controles y procedimientos necesarios para garantizar la seguridad mínima requerida?

	Si	No
a) Procedimiento de llenado de documentos.	( )	(✓)
b) Procedimiento de encendido y apagado de la computadora.	(✓)	( )
c) Reinicialización del equipo en caso de fallas.	(✓)	( )

2. ¿Se cuentan con procedimientos para asegurar que los cambios en aplicaciones se documenten?

	Si	No
a) Se encuentran justificados por medio de requerimientos de los usuarios.	(✓)	( )
b) Se encuentran descritos mencionando el objetivo y función de éstos.	( )	(✓)
c) Se encuentran probados antes de ser implantados formalmente.	( )	(✓)
d) Se tienen en existencia manuales de referencia para el usuario.	( )	(✓)

B) Procesamiento de la información.

3. ¿Se asegura que sólo los responsables de modificar los programas tengan acceso a éstos, explique de que forma?

Si (✓) No ( )

SOLO LOS USUARIOS CUENTAN CON CLAVE DE ACCESO

4. ¿Quién se encarga de efectuar las siguientes modificaciones a programas y aplicaciones?

	Actualización	Eliminación	Consulta	Captura
Los mismos usuarios	(✓)	(✓)	(✓)	(✓)
El encargado (a) de brindar apoyo informático	( )	( )	(✓)	( )
Programadores	( )	( )	( )	( )
Otros	( )	( )	( )	( )

5. ¿Quién es el encargado de dar asistencia para la soluciones de problemas y aplicaciones que usted utiliza?

a) La encargada de apoyo informático. (✓)
b) Usted mismo. (✓)

6. ¿Cuál es el estado que alcanza el o los problemas suscitados en las aplicaciones que utiliza?
a) Resuelto, usted esta trabajando de nuevo, pero el problema aún sigue latente. (✓)
b) Cerrado se han realizado cambios para que ningún otro usuario tenga el mismo problema. ( )

C) Seguridad en archivos.

7. ¿Se cuenta con procedimientos de respaldo de programas fuente, documentación y archivos en operación, mencionelos?

Si (✓) No ( )

En archivos magnéticos y en forme impreso

8. ¿Se encuentra en un lugar distante el almacenamiento de copias de los archivos?

Si ( ) No (✓)

9. ¿Existen bitacoras para tener un control por escrito de las modificaciones hechas a programas y aplicaciones?

Si ( ) No (✓)

"CUESTIONARIO DE ADMINISTRACIÓN DE CAMBIOS Y PROBLEMAS EN APLICACIONES"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Controles y procedimientos utilizados.

1. Se cuenta con controles y procedimientos necesarios para garantizar la seguridad mínima requerida?

	Si	*No*
a) Procedimiento de llenado de documentos.	( )	( )
b) Procedimiento de encendido y apagado de la computadora.	(✓)	( )
c) Reinicialización del equipo en caso de fallas.	(✓)	( )

2. ¿Se cuentan con procedimientos para asegurar que los cambios en aplicaciones se documenten?

	Si	*No*
a) Se encuentran justificados por medio de requerimientos de los usuarios.	( )	( )
b) Se encuentran descritos mencionando el objetivo y función de éstos.	(✓)	( )
c) Se encuentran probados antes de ser implantados formalmente.	( )	( )
d) Se tienen en existencia manuales de referencia para el usuario.	( )	( )

B) Procesamiento de la Información.

3. ¿Se asegura que sólo los responsables de modificar los programas tengan acceso a éstos, explique de que forma?

Si (✓) No ( )

Unicamente el responsable de la información

4. ¿Quien se encarga de efectuar las siguientes modificaciones a programas y aplicaciones?

	Actualización	Eliminación	Consulta	Captura
Los mismos usuarios	( )	( )	( )	( )
El encargado (a) de brindar apoyo informatico	(✓)	(✓)	(✓)	(✓)
Programadores	( )	( )	( )	( )
Otros	( )	( )	( )	( )

5. ¿Quién es el encargado de dar asistencia para la soluciones de problemas y aplicaciones que usted utiliza?

a) La encargada de apoyo informatico. (✓)
b) Usted mismo. ( )

6. ¿Cuál es el estado que alcanza el o los problemas suscitados en las aplicaciones que utiliza?
a) Resuelto, usted está trabajando de nuevo, pero el problema aún sigue latente. ( )
b) Cerrado se han realizado cambios para que ningún otro usuario tenga el mismo problema. (✓)

C) Seguridad en archivos

7. ¿Se cuenta con procedimientos de respaldo de programas fuente, documentación y archivos en operación, mencionelos?

Si ( ) No (✓)

8. ¿Se encuentra en un lugar distante el almacenamiento de copias de los archivos?

Si ( ) No (✓)

9. ¿Existen bitacoras para tener un control por escrito de las modificaciones hechas a programas y aplicaciones?

Si (✓) No ( )

"CUESTIONARIO DE ADMINISTRACIÓN DE CAMBIOS Y PROBLEMAS EN APLICACIONES"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Controles y procedimientos utilizados.

1. Se cuenta con controles y procedimientos necesarios para garantizar la seguridad mínima requerida?

	Si	*No*
a) Procedimiento de llenado de documentos.	( )	(X)
b) Procedimiento de encendido y apagado de la computadora.	( )	(X)
c) Reinicialización del equipo en caso de fallas.	( )	(X)

2. ¿Se cuentan con procedimientos para asegurar que los cambios en aplicaciones se documenten?

	Si	*No*
a) Se encuentran justificados por medio de requerimientos de los usuarios.	( )	(X)
b) Se encuentran descritos mencionando el objetivo y función de éstos.	( )	(X)
c) Se encuentran probados antes de ser implantados formalmente.	( )	(X)
d) Se tienen en existencia manuales de referencia para el usuario.	( )	(X)

B) Procesamiento de la información.

3. ¿Se asegura que sólo los responsables de modificar los programas tengan acceso a estos, explique de que forma?

Si ( ) No (X)

No hay información confidencial a alguien tiene acceso

4. ¿Quien se encarga de efectuar las siguientes modificaciones a programas y aplicaciones?

	Actualización	Eliminación	Consulta	Captura
Los mismos usuarios	( )	( )	( )	( )
El encargado (a) de brindar apoyo informático	(X)	(X)	(X)	(X)
Programadores	(X)	(X)	(X)	(X)
Otros	( )	( )	( )	( )

5. ¿Quien es el encargado de dar asistencia para la soluciones de problemas y aplicaciones que usted utiliza?

a) La encargada de apoyo informático. (X)
b) Usted mismo. ( )

¿Cuál es el estado que alcanza el o los problemas suscitados en las aplicaciones que utiliza?
a) Resuelto, usted está trabajando de nuevo, pero el problema aún sigue latente. ( )
b) Cerrado se han realizado cambios para que ningún otro usuario tenga el mismo problema. (X)

C) Seguridad en archivos.

1. ¿Se cuenta con procedimientos de respaldo de programas fuente, documentación y archivos en operación, mencionelos?

Si (X) No ( )

Respaldos magneticos

2. ¿Se encuentra en un lugar distante el almacenamiento de copias de los archivos?

Si ( ) No (X)

¿Existen bitacoras para tener un control por escrito de las modificaciones hechas a programas y aplicaciones?

Si ( ) No (X)

"CUESTIONARIO DE ADMINISTRACIÓN DE CAMBIOS Y PROBLEMAS EN APLICACIONES"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Controles y procedimientos utilizados.

1. Se cuenta con controles y procedimientos necesarios para garantizar la seguridad mínima requerida?

	Si	*No*
a) Procedimiento de llenado de documentos.	( )	(✓)
b) Procedimiento de encendido y apagado de la computadora.	( )	(✓)
c) Reinicialización del equipo en caso de fallas.	( )	(✓)

2. ¿Se cuentan con procedimientos para asegurar que los cambios en aplicaciones se documenten?

	Si	*No*
a) Se encuentran justificados por medio de requerimientos de los usuarios.	(✓)	( )
b) Se encuentran descritos mencionando el objetivo y función de éstos.	(✓)	( )
c) Se encuentran probados antes de ser implantados formalmente.	( )	(✓)
d) Se tienen en existencia manuales de referencia para el usuario.	(✓)	( )

B) Procesamiento de la información.

3. ¿Se asegura que sólo los responsables de modificar los programas tengan acceso a éstos, explique de que forma?

Si ( ) No (✓)

4. ¿Quién se encarga de efectuar las siguientes modificaciones a programas y aplicaciones?

	Actualización	Eliminación	Consulta	Captura
Los mismos usuarios	(✓)	(✓)	(✓)	(✓)
El encargado (a) de brindar apoyo informatico	( )	( )	( )	( )
Programadores	( )	( )	( )	( )
Otros	( )	( )	( )	( )

5. ¿Quién es el encargado de dar asistencia para la soluciones de problemas y aplicaciones que usted utiliza?

a) La encargada de apoyo informatico. (✓)
b) Usted mismo ( )

6. ¿Cual es el estado que alcanza el o los problemas suscitados en las aplicaciones que utiliza?
a) Resuelto, usted está trabajando de nuevo, pero el problema aún sigue latente. (✓)
b) Cerrado se han realizado cambios para que ningún otro usuario tenga el mismo problema. ( )

C) Seguridad en archivos.

7. ¿Se cuenta con procedimientos de resguardo de programas fuente, documentación y archivos en operación, mencionelos?

Si ( ) No (✓)

8. ¿Se encuentra en un lugar distante el almacenamiento de copias de los archivos?

Si ( ) No (✓)

9. ¿Existen bitacoras para tener un control por escrito de las modificaciones hechas a programas y aplicaciones?

Si ( ) No (✓)

"CUESTIONARIO DE ADMINISTRACIÓN DE CAMBIOS Y PROBLEMAS EN APLICACIONES"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Controles y procedimientos utilizados.

1. Se cuenta con controles y procedimientos necesarios para garantizar la seguridad mínima requerida?

	Si	*No*
a) Procedimiento de llenado de documentos.	(X)	( )
b) Procedimiento de encendido y apagado de la computadora.	(X)	( )
c) Reinicialización del equipo en caso de fallas.	(X)	( )

2. ¿Se cuentan con procedimientos para asegurar que los cambios en aplicaciones se documenten?

	Si	*No*
a) Se encuentran justificados por medio de requerimientos de los usuarios.	( )	(X)
b) Se encuentran descritos mencionando el objetivo y función de éstos.	( )	(X)
c) Se encuentran probados antes de ser implantados formalmente.	( )	(X)
d) Se tienen en existencia manuales de referencia para el usuario.	( )	(X)

B) Procesamiento de la información.

3. ¿Se asegura que sólo los responsables de modificar los programas tengan acceso a éstos, explique de que forma?

Si ( ) No ( )

4. ¿Quién se encarga de efectuar las siguientes modificaciones a programas y aplicaciones?

	Actualización	Eliminación	Consulta	Captura
Los mismos usuarios	( )	( )	( )	( )
El encargado (a) de brindar apoyo informático	(X)	(X)	(X)	(X)
Programadores	( )	( )	( )	( )
Otros	( )	( )	( )	( )

5. ¿Quién es el encargado de dar asistencia para la soluciones de problemas y aplicaciones que usted utiliza?

a) La encargada de apoyo informatico. (X)
b) Usted mismo. ( )

6. ¿Cual es el estado que alcanza el o los problemas suscitados en las aplicaciones que utiliza?
a) Resuelto, usted esta trabajando de nuevo, pero el problema aún sigue latente. (X)
b) Cerrado se han realizado cambios para que ningún otro usuario tenga el mismo problema. (X)

C) Seguridad en archivos.

7. ¿Se cuenta con procedimientos de respaldo de programas fuente, documentación y archivos en operación, menciónelos?

Si ( ) No ( )

8. ¿Se encuentra en un lugar distante el almacenamiento de copias de los archivos?
Si ( ) No (X)
9. ¿Existen bitácoras para tener un control por escrito de las modificaciones hechas a programas y aplicaciones?

Si ( ) No (X)

"CUESTIONARIO DE ADMINISTRACIÓN DE CAMBIOS Y PROBLEMAS EN APLICACIONES"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Controles y procedimientos utilizados.

1. Se cuenta con controles y procedimientos necesarios para garantizar la seguridad mínima requerida?

	Si	*No*
a) Procedimiento de llenado de documentos.	(✓)	( )
b) Procedimiento de encendido y apagado de la computadora.	( )	(✓)
c) Reinicialización del equipo en caso de fallas.	( )	(✓)

2. ¿Se cuentan con procedimientos para asegurar que los cambios en aplicaciones se documenten?

	Si	*No*
a) Se encuentran justificados por medio de requerimientos de los usuarios.	( )	(✓)
b) Se encuentran descritos mencionando el objetivo y función de éstos.	( )	(✓)
c) Se encuentran probados antes de ser implantados formalmente.	(✓)	( )
d) Se tienen en existencia manuales de referencia para el usuario.	( )	(✓)

B) Procesamiento de la información.

3. ¿Se asegura que sólo los responsables de modificar los programas tengan acceso a éstos, explique de que forma?

Si ( ) No (✓)

4. ¿Quién se encarga de efectuar las siguientes modificaciones a programas y aplicaciones?

	Actualización	Eliminación	Consulta	Captura
Los mismos usuarios	( )	( )	( )	( )
El encargado (a) de brindar apoyo informático	( )	( )	( )	( )
Programadores	( )	( )	( )	( )
Otros	( )	( )	( )	( )

5. ¿Quién es el encargado de dar asistencia para la soluciones de problemas y aplicaciones que usted utiliza?

a) La encargada de apoyo informático. (✓)
b) Usted mismo. ( )

6. ¿Cuál es el estado que alcanza el o los problemas suscitados en las aplicaciones que utiliza?
a) Resuelto, usted está trabajando de nuevo, pero el problema aún sigue latente. (✓)
b) Cerrado se han realizado cambios para que ningún otro usuario tenga el mismo problema. ( )

C) Seguridad en archivos.

7. ¿Se cuenta con procedimientos de respaldo de programas fuente, documentación y archivos en operación, mencionelos?

Si ( ) No (✓)

8. ¿Se encuentra en un lugar distante el almacenamiento de copias de los archivos?
Si (✓) No ( )

9. ¿Existen bitácoras para tener un control por escrito de las modificaciones hechas a programas y aplicaciones?

Si ( ) No (✓)

Analisis del Cuestionario sobre Seguridad Lógica

8 cuestionarios aplicados

PREGUNTA 1

Se controla el préstamo de:

RESPUESTAS:

	Elementos magneticos	Equipo	Software
SI	5	4	4
NO		1	1

PREGUNTA 2

Se cuenta con copias de los archivos en un lugar distinto al de la computadora?

RESPUESTAS:

Si	No
4	4

PREGUNTA 3

Se tienen establecidos procedimientos de actualización para estas copias?

RESPUESTAS

Si	No
2	6

PREGUNTA 4

Se elabora un análisis del perfil del usuario para tener acceso a la información?

RESPUESTAS

Si	No
	8

PREGUNTA 5

Existen controles y medidas de seguridad sobre las siguientes operaciones?

RESPUESTAS

	Si	No
Recepcion de documentos	6	2
Informacion confidencial	5	2
Captacion de documentos	4	2
Programas	4	3
Documentos de salida	4	3
Archivos magneticos	3	4

PREGUNTA 6

Existe un responsable de asignación de claves de acceso al equipo?

RESPUESTAS

Si	No
4	4

PREGUNTA 7

Se lleva un control sobre las claves asignadas?

RESPUESTAS

Si	No
4	4

PREGUNTA 8

Existe un cambio periodico en las claves de acceso?

RESPUESTAS

Si	No
2	6

PREGUNTA 9

Existen copias mensuales de archivos históricos de la información?

RESPUESTAS

Si	No
	8

PREGUNTA 10

Existen técnicas de encripción para datos?

RESPUESTAS

Si	No
	8

Analisis del Cuestionario sobre Seguridad Lógica

PREGUNTA 11

Existen registros con información relevante para el administrador de la red, si es así éstos son generados por?

RESPUESTAS

SI	No
1	7

A) ALGUN TIPO DE SOFTWARE

PREGUNTA 12

Se protege el acceso a librerías del sistema?

RESPUESTAS

SI	No
1	5

PREGUNTA 13

Se tiene un control para determinar las rutas de acceso al sistema?

RESPUESTAS

SI	No
2	5

PREGUNTA 14

En lo que se refiere a sistemas de información se cuenta con un campo de validación para accesar a la información?

RESPUESTAS

SI	No
1	5

PREGUNTA 15

Existen controles de acceso al diccionario de datos?

RESPUESTAS

SI	No
	4

PREGUNTA 16

En cuanto al proceso de identificación del usuario:

RESPUESTAS

	SI	No
Se revocan usuarios inactivos	2	1
Se despliega la última fecha en que se accesó		1

"CUESTIONARIO DE SEGURIDAD LÓGICA".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Se controla el préstamo de:
   a) Elementos magnéticos ( )
   b) Equipo ( )
   c) Software ( )
2. ¿Se cuenta con copias de los archivos en un lugar distinto al de la computadora?
   Si (X) No ( )
3. ¿Se tienen establecidos procedimientos de actualización para estas copias?
   Si (X) No ( )
4. ¿Se elabora un análisis del perfil del usuario para tener acceso a la información?
   Si ( ) No (X)
5. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones?

	Si	*No*
a) Recepción de documentos	(X)	( )
b) Información confidencial	(X)	( )
c) Captación de documentos	( )	( )
d) Programas	(X)	( )
e) Documentos de salida	(X)	( )
f) Archivos magnéticos	(X)	( )

6. ¿Existe un responsable de asignación de claves de acceso al equipo?
   Si (X) No ( )
7. ¿Se lleva un control sobre las claves asignadas?
   Si (X) No ( )
8. ¿Existe un cambio periódico en las claves de acceso?
   Si ( ) No (X)
9. Existen copias mensuales de archivos históricos de la información?
   Si ( ) No (X)
10. ¿Existen técnicas de encripción para datos?
    Si ( ) No (X)
11. ¿Existen registros con información relevante para el administrador de la red, si es así Quién los genera?
    Si ( ) No (X)
    a) Algún tipo de software ( )
    b) Por los responsables del sistema ( )
12. ¿Se protege el acceso a librerías del sistema?
    Si ( ) No (X)
13. ¿Se tiene un control para determinar las rutas de acceso al sistema?
    Si ( ) No (X)
14. ¿En lo que se refiere a sistemas de información se cuenta con un campo de validación para acceder a la información?
    Si ( ) No ( )
15. ¿Existen controles de acceso al diccionario de datos?
    Si ( ) No ( )
16. En cuanto al proceso de identificación del usuario:
    a) Se revocan usuarios inactivos ( )
    b) Se despliega la última fecha en que se tiene acceso. ( )

"CUESTIONARIO DE SEGURIDAD LÓGICA".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Se controla el préstamo de:
   a) Elementos magnéticos (✓)
   b) Equipo ( )
   c) Software ( )
2. ¿Se cuenta con copias de los archivos en un lugar distinto al de la computadora?
   Si (✓) No ( )
3. ¿Se tienen establecidos procedimientos de actualización para estas copias?
   Si (✓) No ( )
4. ¿Se elabora un análisis del perfil del usuario para tener acceso a la información?
   Si ( ) No (✓)
5. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones?

	Si	*No*
a) Recepción de documentos	(✓)	( )
b) Información confidencial	(✓)	( )
c) Captación de documentos	( )	( )
d) Programas	(✓)	( )
e) Documentos de salida	(✓)	( )
f) Archivos magnéticos	(✓)	( )

6. ¿Existe un responsable de asignación de claves de acceso al equipo?
   Si (✓) No ( )
7. ¿Se lleva un control sobre las claves asignadas?
   Si (✓) No ( )
8. ¿Existe un cambio periódico en las claves de acceso?
   Si ( ) No (✓)
9. Existen copias mensuales de archivos históricos de la información?
   Si ( ) No (✓)
10. ¿Existen técnicas de encripción para datos?
    Si ( ) No (✓)
11. ¿Existen registros con información relevante para el administrador de la red, si es así Quién los genera?
    Si ( ) No (✓)
    a) Algún tipo de software ( )
    b) Por los responsables del sistema ( )
12. ¿Se protege el acceso a librerías del sistema?
    Si ( ) No (✓)
13. ¿Se tiene un control para determinar las rutas de acceso al sistema?
    Si ( ) No (✓)
14. ¿En lo que se refiere a sistemas de información se cuenta con un campo de validación para acceder a la información?
    Si ( ) No (✓)
15. ¿Existen controles de acceso al diccionario de datos?
    Si ( ) No ( )
16. En cuanto al proceso de identificación del usuario:
    a) Se revocan usuarios inactivos ( )
    b) Se despliega la última fecha en que se tiene acceso. ( )

"CUESTIONARIO DE SEGURIDAD LÓGICA".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Se controla el préstamo de:
   a) Elementos magnéticos ( )
   b) Equipo (X)
   c) Software ( )
2. ¿Se cuenta con copias de los archivos en un lugar distinto al de la computadora?
   Si (X) No ( )
3. ¿Se tienen establecidos procedimientos de actualización para estas copias?
   Si ( ) No (X)
4. ¿Se elabora un análisis del perfil del usuario para tener acceso a la información?
   Si ( ) No (X)
5. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones?

	Si	*No*
a) Recepción de documentos	(X)	( )
b) Información confidencial	( )	( )
c) Captación de documentos	(X)	( )
d) Programas	( )	( )
e) Documentos de salida	( )	( )
f) Archivos magnéticos	( )	( )

6. ¿Existe un responsable de asignación de claves de acceso al equipo?
   Si ( ) No (X)
7. ¿Se lleva un control sobre las claves asignadas?
   Si ( ) No (X)
8. ¿Existe un cambio periódico en las claves de acceso?
   Si ( ) No (X)
9. Existen copias mensuales de archivos históricos de la información?
   Si ( ) No (X)
10. ¿Existen técnicas de encripción para datos?
    Si ( ) No (X)
11. ¿Existen registros con información relevante para el administrador de la red, si es así Quién los genera?
    Si ( ) No (X)
    a) Algún tipo de software ( )
    b) Por los responsables del sistema ( )
12. ¿Se protege el acceso a librerías del sistema?
    Si (X) No ( )
13. ¿Se tiene un control para determinar las rutas de acceso al sistema?
    Si (X) No ( )
14. ¿En lo que se refiere a sistemas de información se cuenta con un campo de validación para acceder a la información?
    Si ( ) No (X)
15. ¿Existen controles de acceso al diccionario de datos?
    Si ( ) No (X)
16. En cuanto al proceso de identificación del usuario:
    a) Se revocan usuarios inactivos (X)
    b) Se despliega la última fecha en que se tiene acceso. ( )

"CUESTIONARIO DE SEGURIDAD LÓGICA".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Se controla el préstamo de:
   a) Elementos magnéticos ( )
   b) Equipo ( )
   c) Software (✓)
2. ¿Se cuenta con copias de los archivos en un lugar distinto al de la computadora?
   Si ( ) No ( )
3. ¿Se tienen establecidos procedimientos de actualización para estas copias?
   Si ( ) No (✓)
4. ¿Se elabora un análisis del perfil del usuario para tener acceso a la información?
   Si ( ) No (✓)
5. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones?

	Si	*No*
a) Recepción de documentos	( )	(✓)
b) Información confidencial	( )	(✓)
c) Captación de documentos	( )	(✓)
d) Programas	( )	(✓)
e) Documentos de salida	( )	(✓)
f) Archivos magnéticos	( )	(✓)

6. ¿Existe un responsable de asignación de claves de acceso al equipo?
   Si ( ) No (✓)
7. ¿Se lleva un control sobre las claves asignadas?
   Si ( ) No (✓)
8. ¿Existe un cambio periódico en las claves de acceso?
   Si ( ) No (✓)
9. Existen copias mensuales de archivos históricos de la información?
   Si ( ) No ( )
10. ¿Existen técnicas de encripción para datos?
    Si ( ) No (✓)
11. ¿Existen registros con información relevante para el administrador de la red, si es así Quién los genera?
    Si ( ) No (✓)
    a) Algún tipo de software ( )
    b) Por los responsables del sistema (✓)
12. ¿Se protege el acceso a librerías del sistema?
    Si ( ) No (✓)
13. ¿Se tiene un control para determinar las rutas de acceso al sistema?
    Si ( ) No (✓)
14. ¿En lo que se refiere a sistemas de información se cuenta con un campo de validación para acceder a la información?
    Si ( ) No (✓)
15. ¿Existen controles de acceso al diccionario de datos?
    Si ( ) No (✓)
16. En cuanto al proceso de identificación del usuario:
    a) Se revocan usuarios inactivos (✓)
    b) Se despliega la última fecha en que se tiene acceso. ( )

"CUESTIONARIO DE SEGURIDAD LÓGICA".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Se controla el préstamo de:
   a) Elementos magnéticos (X)
   b) Equipo (X)
   c) Software (X)
2. ¿Se cuenta con copias de los archivos en un lugar distinto al de la computadora?
   Si ( ) No (X)
3. ¿Se tienen establecidos procedimientos de actualización para estas copias?
   Si ( ) No (X)
4. ¿Se elabora un análisis del perfil del usuario para tener acceso a la información?
   Si ( ) No (X)
5. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones?

	Si	*No*
a) Recepción de documentos	(X)	( )
b) Información confidencial	(X)	( )
c) Captación de documentos	(X)	( )
d) Programas	(X)	( )
e) Documentos de salida	(X)	( )
f) Archivos magnéticos	( )	(X)

6. ¿Existe un responsable de asignación de claves de acceso al equipo?
   Si (X) No ( )
7. ¿Se lleva un control sobre las claves asignadas?
   Si (X) No ( )
8. ¿Existe un cambio periódico en las claves de acceso?
   Si (X) No ( )
9. Existen copias mensuales de archivos históricos de la información?
   Si ( ) No (X)
10. ¿Existen técnicas de encripción para datos?
    Si ( ) No (X)
11. ¿Existen registros con información relevante para el administrador de la red, si es así Quién los genera?
    Si ( ) No (X)
    a) Algún tipo de software ( )
    b) Por los responsables del sistema ( )
12. ¿Se protege el acceso a librerías del sistema?
    Si ( ) No ( )
13. ¿Se tiene un control para determinar las rutas de acceso al sistema?
    Si (X) No ( )
14. ¿En lo que se refiere a sistemas de información se cuenta con un campo de validación para acceder a la información?
    Si ( ) No ( )
15. ¿Existen controles de acceso al diccionario de datos?
    Si ( ) No ( )
16. En cuanto al proceso de identificación del usuario:
    a) Se revocan usuarios inactivos ( )
    b) Se despliega la última fecha en que se tiene acceso. ( )

"CUESTIONARIO DE SEGURIDAD LÓGICA".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Se controla el préstamo de:
   a) Elementos magnéticos (✓)
   b) Equipo (✓)
   c) Software (✓)
2. ¿Se cuenta con copias de los archivos en un lugar distinto al de la computadora?
   Si ( ) No (✓)
3. ¿Se tienen establecidos procedimientos de actualización para estas copias?
   Si ( ) No (✓)
4. ¿Se elabora un análisis del perfil del usuario para tener acceso a la información?
   Si ( ) No (✓)
5. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones?

	Si	*No*
a) Recepción de documentos	(✓)	( )
b) Información confidencial	(✓)	( )
c) Captación de documentos	(✓)	( )
d) Programas	(✓)	( )
e) Documentos de salida	(✓)	( )
f) Archivos magnéticos	( )	(✓)

6. ¿Existe un responsable de asignación de claves de acceso al equipo?
   Si (✓) No ( )
7. ¿Se lleva un control sobre las claves asignadas?
   Si (✓) No ( )
8. ¿Existe un cambio periódico en las claves de acceso?
   Si (✓) No ( )
9. Existen copias mensuales de archivos históricos de la información?
   Si ( ) No (✓)
10. ¿Existen técnicas de encripción para datos?
    Si ( ) No (✓)
11. ¿Existen registros con información relevante para el administrador de la red, si es así Quién los genera?
    Si ( ) No (✓)
    a) Algún tipo de software ( )
    b) Por los responsables del sistema ( )
12. ¿Se protege el acceso a librerías del sistema?
    Si ( ) No ( )
13. ¿Se tiene un control para determinar las rutas de acceso al sistema?
    Si (✓) No ( )
14. ¿En lo que se refiere a sistemas de información se cuenta con un campo de validación para acceder a la información?
    Si (✓) No ( )
15. ¿Existen controles de acceso al diccionario de datos?
    Si ( ) No ( )
16. En cuanto al proceso de identificación del usuario:
    a) Se revocan usuarios inactivos ( )
    b) Se despliega la última fecha en que se tiene acceso. ( )

"CUESTIONARIO DE SEGURIDAD LÓGICA".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Se controla el préstamo de:
   a) Elementos magnéticos (X)
   b) Equipo (X)
   c) Software ( )
2. ¿Se cuenta con copias de los archivos en un lugar distinto al de la computadora?
   Si ( ) No (X)
3. ¿Se tienen establecidos procedimientos de actualización para estas copias?
   Si ( ) No (X)
4. ¿Se elabora un análisis del perfil del usuario para tener acceso a la información?
   Si ( ) No (X)
5. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones?

	Si	*No*
a) Recepción de documentos	( )	(X)
b) Información confidencial	(X)	( )
c) Captación de documentos	( )	(X)
d) Programas	( )	(X)
e) Documentos de salida	( )	(X)
f) Archivos magnéticos	( )	(X)

6. ¿Existe un responsable de asignación de claves de acceso al equipo?
   Si ( ) No (X)
7. ¿Se lleva un control sobre las claves asignadas?
   Si ( ) No (X)
8. ¿Existe un cambio periódico en las claves de acceso?
   Si ( ) No (X)
9. Existen copias mensuales de archivos históricos de la información?
   Si ( ) No (X)
10. ¿Existen técnicas de encripción para datos?
    Si ( ) No (X)
11. ¿Existen registros con información relevante para el administrador de la red, si es así Quién los genera?
    Si ( ) No (X)
    a) Algún tipo de software ( )
    b) Por los responsables del sistema ( )
12. ¿Se protege el acceso a librerías del sistema?
    Si ( ) No (X)
13. ¿Se tiene un control para determinar las rutas de acceso al sistema?
    Si ( ) No (X)
14. ¿En lo que se refiere a sistemas de información se cuenta con un campo de validación para acceder a la información?
    Si ( ) No (X)
15. ¿Existen controles de acceso al diccionario de datos?
    Si ( ) No (X)
16. En cuanto al proceso de identificación del usuario:
    a) Se revocan usuarios inactivos ( )
    b) Se despliega la última fecha en que se tiene acceso. ( )

"CUESTIONARIO DE SEGURIDAD LÓGICA".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Se controla el préstamo de:
   a) Elementos magnéticos (✓)
   b) Equipo ( )
   c) Software (✓)
2. ¿Se cuenta con copias de los archivos en un lugar distinto al de la computadora?
   Si ( ) No (✓)
3. ¿Se tienen establecidos procedimientos de actualización para estas copias?
   Si ( ) No (✓)
4. ¿Se elabora un análisis del perfil del usuario para tener acceso a la información?
   Si ( ) No (✓)
5. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones?

	Si	*No*
a) Recepción de documentos	(✓)	( )
b) Información confidencial	( )	(✓)
c) Captación de documentos	(✓)	( )
d) Programas	( )	(✓)
e) Documentos de salida	( )	(✓)
f) Archivos magnéticos	(✓)	( )

6. ¿Existe un responsable de asignación de claves de acceso al equipo?
   Si ( ) No (✓)
7. ¿Se lleva un control sobre las claves asignadas?
   Si ( ) No (✓)
8. ¿Existe un cambio periódico en las claves de acceso?
   Si ( ) No (✓)
9. Existen copias mensuales de archivos históricos de la información?
   Si ( ) No (✓)
10. ¿Existen técnicas de encripción para datos?
    Si ( ) No (✓)
11. ¿Existen registros con información relevante para el administrador de la red, si es así Quién los genera?
    Si (✓) No ( )
    a) Algún tipo de software (✓)
    b) Por los responsables del sistema ( )
12. ¿Se protege el acceso a librerías del sistema?
    Si ( ) No (✓)
13. ¿Se tiene un control para determinar las rutas de acceso al sistema?
    Si ( ) No (✓)
14. ¿En lo que se refiere a sistemas de información se cuenta con un campo de validación para acceder a la información?
    Si ( ) No (✓)
15. ¿Existen controles de acceso al diccionario de datos?
    Si ( ) No (✓)
16. En cuanto al proceso de identificación del usuario:
    a) Se revocan usuarios inactivos ( ) NO
    b) Se despliega la última fecha en que se tiene acceso. ( ) NO

Analisis del Cuestionario sobre la verificación de la Seguridad Cliente / Servidor

8.cuestionarios aplicados

PREGUNTA 1

Cuantas estaciones de trabajo existen en la red?

RESPUESTAS:

encuestado 1	13	encuestado 5	
encuestado 2		encuestado 6	4
encuestado 3		encuestado 7	1
encuestado 4		encuestado 8	

PREGUNTA 2

Con que tipo de servidor se cuenta ?

RESPUESTAS:

a) Dedicado
b) No dedicado

a)	b)
5	2

PREGUNTA 3

Se hace uso del servidor como cliente cuando realiza una solicitud de servicio a otras plataformas dentro de la red?

RESPUESTAS:

Si	No
3	4

PREGUNTA 4

Se ha escalado la infraestructura de la red?

RESPUESTAS:

Si	No
1	7

PREGUNTA 5

Que proyectos se tienen para el crecimiento de la infraestructura computacional?

RESPUESTAS:

- Actualización de la Red Informatica actual y crecimiento de la misma
- Instalar mas puestos de trabajo
  Instalar otro servidor
  Conectar los servidores con F.O. a toda la Red del Metro
- Mantto. Mayor Férreo
- Implantación de un gestor de Mantto.
- Ampliar la capacidad de memoria

PREGUNTA 6

Se han presentado alguno de éstos problemas:

RESPUESTAS:

congestionamiento de la red	Dificultad para el tráfico de los datos
3	6

PREGUNTA 7

Ha habido migración de aplicaciones a otras plataformas?

RESPUESTAS:

Si	No
1	7

Analisis del Cuestionario sobre la verificación de la Seguridad Cliente / Servidor

PREGUNTA 8

Existe algún tipo de control ya sea físico, lógico o administrativo para los datos usados en las PC para reforzar la seguridad de acceso?

RESPUESTAS:

Si	No
4	4

PREGUNTA 9

Existe un responsable encargado de mantener la integridad de los datos y aplicaciones distribuidas en red?

RESPUESTAS:

Si	No
4	4

PREGUNTA 10

Se establecen políticas y procedimientos de seguridad en el servidor, así como en las estaciones de trabajo?

RESPUESTAS:

Si	No
4	3

PREGUNTA 11

El sistema de red LAN soporta las aplicaciones de alto procesamiento transaccional?

RESPUESTAS:

Si	No
3	4

PREGUNTA 12

Comparte algunos de los siguientes servicios de datos e impresión?

RESPUESTAS:

Archivos	8
Bases de datos	4
Impresoras	3
Ploters	
Administración de colas de impresión en diferentes dispositivos	

PREGUNTA 13

Que tipo de protocolo utiliza la red?

RESPUESTAS:

TCP/IP

PREGUNTA 14

Se permite la transportación de aplicaciones de un procesador a otro, si que este se modifique?

RESPUESTAS:

Si	No
4	4

"CUESTIONARIO PARA VERIFICAR LA SEGURIDAD CLIENTE-SERVIDOR"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Cuantas estaciones de trabajo existen en la red? 13
2. ¿Con que tipo de servidor se cuenta?
   a) Dedicado (X)
   b) No dedicado ( )
3. ¿Se hace uso del servidor como cliente cuando realiza una solicitud de servicio a otras plataformas dentro de la red?
   Si (X) No ( )
4. ¿Se ha escalado la infraestructura de la red?
   Si ( ) No (X)
5. ¿Qué proyectos se tienen contemplados para el crecimiento de la infraestructura computacional?
   Actualización de la Red Informática actual y Crecimiento de la misma
6. Se han presentado alguno de éstos problemas:
   a) Congestionamiento en la red. (X)
   b) Dificultad para el tráfico de los datos. ( )
7. ¿Ha habido migración de aplicaciones a otras plataformas?
   Si ( ) No (X)
8. ¿Existe algún tipo de control ya sea físico, lógico o administrativo para los datos usados en las PC para reforzar la seguridad de acceso.
   Si ( ) No (X)
9. ¿Existe un responsable encargado de mantener la integridad de los datos y aplicaciones distribuidas en red?
   Si ( ) No (X)
10. ¿Se establecen políticas y procedimientos de seguridad en el servidor, así como en las estaciones de trabajo?
    Si (X) No ( )
11. ¿El sistema de red LAN soporta las aplicaciones de alto procesamiento transaccional?
    Si ( ) No (X)
12. ¿Qué servicios de datos e impresión comparte?
    a) Archivos (X)
    b) Base de datos (X)
    c) Impresoras (X)
    d) Plotters ( )
    e) Administración de colas de impresión en diferentes dispositivos ( )

13. ¿Qué tipo de protocolo utiliza la red? TCP/IP
14. ¿Se permite la transportación de aplicaciones de un procesador a otro, sin que éste se modifique?
    Si (X) No ( )

"CUESTIONARIO PARA VERIFICAR LA SEGURIDAD CLIENTE-SERVIDOR"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Cuantas estaciones de trabajo existen en la red? 13
2. ¿Con que tipo de servidor se cuenta?
   a) Dedicado ( )
   b) No dedicado (X)
3. ¿Se hace uso del servidor como cliente cuando realiza una solicitud de servicio a otras plataformas dentro de la red?
   Si ( ) No ( )
4. ¿Se ha escalado la infraestructura de la red?
   Si ( ) No (X)
5. ¿Qué proyectos se tienen contemplados para el crecimiento de la infraestructura computacional?
   NO TENGO CONOCIMIENTO
6. Se han presentado alguno de éstos problemas:
   a) Congestionamiento en la red. ( )
   b) Dificultad para el tráfico de los datos. ( )
7. ¿Ha habido migración de aplicaciones a otras plataformas?
   Si ( ) No (X)
8. ¿Existe algún tipo de control ya sea físico, lógico o administrativo para los datos usados en las PC para reforzar la seguridad de acceso.
   Si (X) No ( )
9. ¿Existe un responsable encargado de mantener la integridad de los datos y aplicaciones distribuidas en red?
   Si (X) No ( )
10. ¿Se establecen políticas y procedimientos de seguridad en el servidor, así como en las estaciones de trabajo?
    Si (X) No ( )
11. ¿El sistema de red LAN soporta las aplicaciones de alto procesamiento transaccional?
    Si ( ) No ( )
12. ¿Qué servicios de datos e impresión comparte?
    a) Archivos (X)
    b) Base de datos ( )
    c) Impresoras ( )
    d) Plotters ( )
    e) Administración de colas de impresión en diferentes dispositivos ( )
13. ¿Qué tipo de protocolo utiliza la red?
14. ¿Se permite la transportación de aplicaciones de un procesador a otro, sin que éste se modifique?
    Si (X) No ( )

"CUESTIONARIO PARA VERIFICAR LA SEGURIDAD CLIENTE-SERVIDOR"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Cuantas estaciones de trabajo existen en la red? 13
2. ¿Con que tipo de servidor se cuenta?
   a) Dedicado ( )
   b) No dedicado (✓)
3. ¿Se hace uso del servidor como cliente cuando realiza una solicitud de servicio a otras plataformas dentro de la red?
   Si ( ) No (✓)
4. ¿Se ha escalado la infraestructura de la red?
   Si ( ) No (✓)
5. ¿Qué proyectos se tienen contemplados para el crecimiento de la infraestructura computacional? _____
6. Se han presentado alguno de éstos problemas:
   a) Congestionamiento en la red. ( )
   b) Dificultad para el tráfico de los datos. (✓)
7. ¿Ha habido migración de aplicaciones a otras plataformas?
   Si ( ) No (✓)
8. ¿Existe algún tipo de control ya sea físico, lógico o administrativo para los datos usados en las PC para reforzar la seguridad de acceso.
   Si ( ) No (✓)
9. ¿Existe un responsable encargado de mantener la integridad de los datos y aplicaciones distribuidas en red?
   Si (✓) No ( )
10. ¿Se establecen políticas y procedimientos de seguridad en el servidor, así como en las estaciones de trabajo?
    Si (✓) No ( )
11. ¿El sistema de red LAN soporta las aplicaciones de alto procesamiento transaccional?
    Si (✓) No ( )
12. ¿Qué servicios de datos e impresión comparte?
    a) Archivos (✓)
    b) Base de datos ( )
    c) Impresoras (✓)
    d) Plotters ( )
    e) Administración de colas de impresión en diferentes dispositivos ( )
13. ¿Que tipo de protocolo utiliza la red?_____
14. ¿Se permite la transportación de aplicaciones de un procesador a otro, sin que este se modifique?
    Si ( ) No (✓)

"CUESTIONARIO PARA VERIFICAR LA SEGURIDAD CLIENTE-SERVIDOR"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Cuantas estaciones de trabajo existen en la red? 13
2. ¿Con que tipo de servidor se cuenta?
   a) Dedicado (X)
   b) No dedicado ( )
3. ¿Se hace uso del servidor como cliente cuando realiza una solicitud de servicio a otras plataformas dentro de la red?
   Si (X) No ( )
4. ¿Se ha escalado la infraestructura de la red?
   Si ( ) No (X)
5. ¿Qué proyectos se tienen contemplados para el crecimiento de la infraestructura computacional? _____
6. Se han presentado alguno de éstos problemas:
   a) Congestionamiento en la red. (X)
   b) Dificultad para el tráfico de los datos. (X)
7. ¿Ha habido migración de aplicaciones a otras plataformas?
   Si ( ) No (X)
8. ¿Existe algún tipo de control ya sea físico, lógico o administrativo para los datos usados en las PC para reforzar la seguridad de acceso.
   Si ( ) No (X)
9. ¿Existe un responsable encargado de mantener la integridad de los datos y aplicaciones distribuidas en red?
   Si ( ) No (X)
10. ¿Se establecen políticas y procedimientos de seguridad en el servidor, así como en las estaciones de trabajo?
    Si ( ) No (X)
11. ¿El sistema de red LAN soporta las aplicaciones de alto procesamiento transaccional?
    Si (X) No ( )
12. ¿Qué servicios de datos e impresión comparte?
    a) Archivos (X)
    b) Base de datos ( )
    c) Impresoras ( )
    d) Plotters ( )
    e) Administración de colas de impresión en diferentes dispositivos ( )
13. ¿Qué tipo de protocolo utiliza la red?_____
14. ¿Se permite la transportación de aplicaciones de un procesador a otro, sin que éste se modifique?
    Si ( ) No (X)

"CUESTIONARIO PARA VERIFICAR LA SEGURIDAD CLIENTE-SERVIDOR"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Cuantas estaciones de trabajo existen en la red? 13
2. ¿Con que tipo de servidor se cuenta?
   a) Dedicado (✓)
   b) No dedicado ( )
3. ¿Se hace uso del servidor como cliente cuando realiza una solicitud de servicio a otras plataformas dentro de la red?
   Si ( ) No (✓)
4. ¿Se ha escalado la infraestructura de la red?
   Si ( ) No (✓)
5. ¿Qué proyectos se tienen contemplados para el crecimiento de la infraestructura computacional? Instalación de más nodos de trabajo
   Instalacion de otro servidor
   Conectar los servidores por medio de fibra optica Red global.
6. Se han presentado alguno de éstos problemas:
   a) Congestionamiento en la red. ( )
   b) Dificultad para el tráfico de los datos. (✓)
7. ¿Ha habido migración de aplicaciones a otras plataformas?
   Si ( ) No (✓)
8. ¿Existe algún tipo de control ya sea físico, lógico o administrativo para los datos usados en las PC para reforzar la seguridad de acceso.
   Si (✓) No ( )
9. ¿Existe un responsable encargado de mantener la integridad de los datos y aplicaciones distribuidas en red?
   Si (✓) No ( )
10. ¿Se establecen políticas y procedimientos de seguridad en el servidor, así como en las estaciones de trabajo?
    Si ( ) No (✓)
11. ¿El sistema de red LAN soporta las aplicaciones de alto procesamiento transaccional?
    Si ( ) No (✓)
12. ¿Qué servicios de datos e impresión comparte?
    a) Archivos (✓)
    b) Base de datos ( )
    c) Impresoras (✓)
    d) Plotters ( )
    e) Administración de colas de impresión en diferentes dispositivos ( )
13. ¿Qué tipo de protocolo utiliza la red?_____
14. ¿Se permite la transportación de aplicaciones de un procesador a otro, sin que éste se modifique?
    Si (✓) No ( )

"CUESTIONARIO PARA VERIFICAR LA SEGURIDAD CLIENTE-SERVIDOR"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Cuantas estaciones de trabajo existen en la red? 13
2. ¿Con que tipo de servidor se cuenta?
   a) Dedicado (X)
   b) No dedicado ( )
3. ¿Se hace uso del servidor como cliente cuando realiza una solicitud de servicio a otras plataformas dentro de la red?
   Si ( ) No (X)
4. ¿Se ha escalado la infraestructura de la red?
   Si ( ) No (X)
5. ¿Qué proyectos se tienen contemplados para el crecimiento de la infraestructura computacional?
   PROYECTO PARA EL MANTTO. MAYOR
6. Se han presentado alguno de éstos problemas:
   a) Congestionamiento en la red. ( )
   b) Dificultad para el tráfico de los datos. (X)
7. ¿Ha habido migración de aplicaciones a otras plataformas?
   Si ( ) No (X)
8. ¿Existe algún tipo de control ya sea físico, lógico o administrativo para los datos usados en las PC para reforzar la seguridad de acceso.
   Si (X) No ( )
9. ¿Existe un responsable encargado de mantener la integridad de los datos y aplicaciones distribuidas en red?
   Si (X) No ( )
10. ¿Se establecen políticas y procedimientos de seguridad en el servidor, así como en las estaciones de trabajo?
    Si ( ) No (X)
11. ¿El sistema de red LAN soporta las aplicaciones de alto procesamiento transaccional?
    Si (X) No ( )
12. ¿Qué servicios de datos e impresión comparte?
    a) Archivos (X)
    b) Base de datos (X)
    c) Impresoras ( )
    d) Plotters ( )
    e) Administración de colas de impresión en diferentes dispositivos ( )
13. ¿Qué tipo de protocolo utiliza la red?_____
14. ¿Se permite la transportación de aplicaciones de un procesador a otro, sin que éste se modifique?
    Si (X) No ( )

"CUESTIONARIO PARA VERIFICAR LA SEGURIDAD CLIENTE-SERVIDOR"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Cuantas estaciones de trabajo existen en la red? 13
2. ¿Con que tipo de servidor se cuenta?
   a) Dedicado (✓)
   b) No dedicado ( )
3. ¿Se hace uso del servidor como cliente cuando realiza una solicitud de servicio a otras plataformas dentro de la red?
   Si (✓) No ( )
4. ¿Se ha escalado la infraestructura de la red?
   Si (✓) No ( )
5. ¿Qué proyectos se tienen contemplados para el crecimiento de la infraestructura computacional?
   IMPLANTACION DE UN GESTOR DE MANTENIMIENTO
6. Se han presentado alguno de éstos problemas:
   a) Congestionamiento en la red. (✓)
   b) Dificultad para el tráfico de los datos. (✓)
7. ¿Ha habido migración de aplicaciones a otras plataformas?
   Si (✓) No ( )
8. ¿Existe algún tipo de control ya sea físico, lógico o administrativo para los datos usados en las PC para reforzar la seguridad de acceso.
   Si ( ) No (✓)
9. ¿Existe un responsable encargado de mantener la integridad de los datos y aplicaciones distribuidas en red?
   Si ( ) No (✓)
10. ¿Se establecen políticas y procedimientos de seguridad en el servidor, así como en las estaciones de trabajo?
    Si ( ) No (✓)
11. ¿El sistema de red LAN soporta las aplicaciones de alto procesamiento transaccional?
    Si ( ) No (✓)
12. ¿Qué servicios de datos e impresión comparte?
    a) Archivos (✓)
    b) Base de datos (✓)
    c) Impresoras ( )
    d) Plotters ( )
    e) Administración de colas de impresión en diferentes dispositivos ( )
13. ¿Qué tipo de protocolo utiliza la red?_____
14. ¿Se permite la transportación de aplicaciones de un procesador a otro, sin que éste se modifique?
    Si ( ) No (✓)

"CUESTIONARIO PARA VERIFICAR LA SEGURIDAD CLIENTE-SERVIDOR"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Cuantas estaciones de trabajo existen en la red? 13
2. ¿Con que tipo de servidor se cuenta?
   a) Dedicado ( )
   b) No dedicado (✓)
3. ¿Se hace uso del servidor como cliente cuando realiza una solicitud de servicio a otras plataformas dentro de la red?
   Si ( ) No (✓)
4. ¿Se ha escalado la infraestructura de la red?
   Si ( ) No (✓)
5. ¿Qué proyectos se tienen contemplados para el crecimiento de la infraestructura computacional?
   Instalación de un Gestor de Mantenimiento
   Ampliar la capacidad de memorias
6. Se han presentado alguno de éstos problemas:
   a) Congestionamiento en la red. ( )
   b) Dificultad para el tráfico de los datos. (✓)
7. ¿Ha habido migración de aplicaciones a otras plataformas?
   Si ( ) No (✓)
8. ¿Existe algún tipo de control ya sea físico, lógico o administrativo para los datos usados en las PC para reforzar la seguridad de acceso.
   Si (✓) No ( )
9. ¿Existe un responsable encargado de mantener la integridad de los datos y aplicaciones distribuidas en red?
   Si ( ) No (✓)
10. ¿Se establecen políticas y procedimientos de seguridad en el servidor, así como en las estaciones de trabajo?
    Si (✓) No ( )
11. ¿El sistema de red LAN soporta las aplicaciones de alto procesamiento transaccional?
    Si ( ) No (✓)
12. ¿Qué servicios de datos e impresión comparte?
    a) Archivos (✓)
    b) Base de datos (✓)
    c) Impresoras ( )
    d) Plotters ( )
    e) Administración de colas de impresión en diferentes dispositivos ( )
13. ¿Qué tipo de protocolo utiliza la red?_____
14. ¿Se permite la transportación de aplicaciones de un procesador a otro, sin que éste se modifique?
    Si ( ) No (✓)

Analisis del Cuestionario sobre la Administración de la Seguridad

8_cuestionarios_aplicados

PREGUNTA 1

Existe una función de investigación dedicada a la evaluación de software, métodos y procedimientos sugeridos en el mercado para la implantación de acciones relativas a la seguridad que brinden un cuidado a los recursos relacionados con la información?

RESPUESTAS:

Si	No
4	6

PREGUNTA 2

EXISTE UNA ADMINISTRACIÓN FORMAL DE LA RED?

RESPUESTAS:

Si	No
2	6

PREGUNTA 3

En caso de no tener una administración formal de la red, ¿Se da el seguimiento a los siguientes aspectos?

RESPUESTAS:

	Si	No
Planeación de nueva tecnología de la información (HW y SW)		7
Monitoreo de las actividades de la operación y mantenimiento de la red	1	6
Procedimientos y control de seguridad		7
Aspectos legales del Software instalado	4	3
Capacitación y soporte a usuarios	1	6

PREGUNTA 4

Algun personal externo interviene en la administración anteriormente mencionada?

RESPUESTAS:

Si	No
4	4

PREGUNTA 5

Existe la documentación formal que especifique que hacer y cómo efectuar las funciones administrativas de la red?

RESPUESTAS:

Si	No
1	7

PREGUNTA 6

Se elaboran políticas y procedimientos de seguridad en cuanto lo que son datos, aplicaciones, hardware, software y accesorios de la red?

RESPUESTAS:

Si	No
	8

PREGUNTA 7

Como se canalizan las dudas, sugerencias y compromisos entre usuarios y responsables de la red?

RESPUESTAS:

Via telefonica o comunicación directa
De forma verbal

PREGUNTA 8

Existe una persona encargada de administrar la red?

RESPUESTAS:

Si	No
6	2

PREGUNTA 9

Se tiene un control en cuanto al numero de horas en las que los usuarios inician sesiones en la red?

RESPUESTAS:

Si	No
	8

Analisis del Cuestionario sobre la Administración de la Seguridad

PREGUNTA 10

Existen estrategias de organización para usuarios o grupos de usuarios?

RESPUESTAS:

Si	No
1	7

PREGUNTA 11

Se tiene implementado algun plan de cuentas para proteger la red?

RESPUESTAS:

Si	No
2	6

PREGUNTA 12

En caso de contar con carpetas compartidas existe una jerarquía en estas?

RESPUESTAS:

Si	No
	8

PREGUNTA 13

Se controla el acceso a aplicaciones y datos?

RESPUESTAS:

Si	No
1	6

PREGUNTA 14

Se han organizado los recursos de disco a fin de que las carpetas que tengan los mismos requisitos de seguridad se ubiquen dentro de la misma jerarquía?

RESPUESTAS:

Si	No
1	6

PREGUNTA 15

Se ha documentado que usuarios y permisos se tienen para acceder recursos?

RESPUESTAS:

Si	No
1	7

PREGUNTA 16

Se han establecido directivas de seguridad para asignar permisos de impresión?

RESPUESTAS:

Si	No
1	7

PREGUNTA 16

Se han contemplado planes de auditoria para archivos, directorios, impresoras y controladores de dominio?

RESPUESTAS:

Si	No
3	5

"CUESTIONARIO DE ADMINISTRACIÓN DE LA SEGURIDAD"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Existe una función de investigación dedicada a la evaluación de software, métodos y procedimientos sugeridos en el mercado para la implantación de acciones relativas a la seguridad que brinden un cuidado a los recursos relacionados con la informática?
   Si (X) No ( )
2. ¿Existe administración formal de la red?
   Si ( ) No (X)
3. ¿En caso de no tener una administración formal de la red, ¿Se da el seguimiento a los siguientes aspectos?

	Si	*No*
a) Planeación de nueva tecnología de la información (hardware y software)	( )	(X)
b) Monitoreo de las actividades de la operación y mantenimiento de la red	(X)	( )
c) Procedimientos y control de seguridad	( )	(X)
d) Aspectos legales del software instalado	(X)	( )
e) Capacitación y soporte a usuarios	(X)	( )

4. ¿Existe alguna persona externa que intervenga en la administración de la red?
   Si (X) No ( )
5. ¿Existe la documentación formal que especifique qué hacer y cómo efectuar las funciones administrativas de la red?
   Si ( ) No (X)
6. ¿Se elaboran políticas y procedimientos de seguridad referente a datos, aplicaciones, hardware, software y accesorios de la red?
   Si ( ) No (X)
7. ¿Cómo se canalizan las dudas, sugerencias y compromisos entre usuarios y responsables de la red? VIA TELEFONICA O COMUNICACION DIRECTA
8. ¿Existe una persona encargada de administrar la red?
   Si ( ) No (X)
9. ¿Se tiene un control en cuanto al número de horas en las que los usuarios inicien sesiones en la red? Si ( ) No (X)
10. ¿Existen estrategias de organización para usuarios o grupos de usuarios?
    Si ( ) No (X)
11. Se tiene implementado algún plan de cuentas para proteger la red?
    Si ( ) No (X)
12. En el caso de contar con carpetas compartidas existe una jerarquía en estas?
    Si ( ) No (X)
13. Se controla el acceso a aplicaciones y datos?
    Si ( ) No (X)
14. Se han organizado los recursos de disco a fin de que las carpetas que tengan los mismos requisitos de seguridad se ubiquen dentro de una misma jerarquía?
    Si (X) No ( )
15. Se ha documentado que usuarios y permisos se tienen para acceder recursos?
    Si ( ) No (X)
16. Se han establecido directivas de seguridad para asignar permisos de impresión?
    Si (X) No ( )
17. Se han contemplado planes de auditoría para archivos, directorios, impresoras y controladores de dominio?
    Si (X) No ( )

"CUESTIONARIO DE ADMINISTRACIÓN DE LA SEGURIDAD"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Existe una función de investigación dedicada a la evaluación de software, métodos y procedimientos sugeridos en el mercado para la implantación de acciones relativas a la seguridad que brinden un cuidado a los recursos relacionados con la informática?
   Si ( ) No (X)
2. ¿Existe administración formal de la red?
   Si ( ) No (X)
3. ¿En caso de no tener una administración formal de la red, ¿Se da el seguimiento a los siguientes aspectos?

	Si	*No*
a) Planeación de nueva tecnología de la información (hardware y software)	( )	(X)
b) Monitoreo de las actividades de la operación y mantenimiento de la red	( )	(X)
c) Procedimientos y control de seguridad	( )	(X)
d) Aspectos legales del software instalado	( )	(X)
e) Capacitación y soporte a usuarios	( )	(X)

4. ¿Existe alguna persona externa que intervenga en la administración de la red?
   Si ( ) No (X)
5. ¿Existe la documentación formal que especifique qué hacer y cómo efectuar las funciones administrativas de la red?
   Si ( ) No (X)
6. ¿Se elaboran políticas y procedimientos de seguridad referente a datos, aplicaciones, hardware, software y accesorios de la red?
   Si ( ) No (X)
7. ¿Cómo se canalizan las dudas, sugerencias y compromisos entre usuarios y responsables de la red? DIRECTAMENTE DE FORMA VERBAL
8. ¿Existe una persona encargada de administrar la red?
   Si (X) No ( )
9. ¿Se tiene un control en cuanto al número de horas en las que los usuarios inicien sesiones en la red? Si ( ) No (X)
10. ¿Existen estrategias de organización para usuarios o grupos de usuarios?
    Si (X) No ( )
11. ¿Se tiene implementado algún plan de cuentas para proteger la red?
    Si (X) No ( )
12. ¿En el caso de contar con carpetas compartidas existe una jerarquía en estas?
    Si ( ) No (X)
13. ¿Se controla el acceso a aplicaciones y datos?
    Si ( ) No ( )
14. ¿Se han organizado los recursos de disco a fin de que las carpetas que tengan los mismos requisitos de seguridad se ubiquen dentro de una misma jerarquía?
    Si ( ) No ( )
15. ¿Se ha documentado que usuarios y permisos se tienen para acceder recursos?
    Si ( ) No (X)
16. ¿Se han establecido directivas de seguridad para asignar permisos de impresión?
    Si ( ) No (X)
17. ¿Se han contemplado planes de auditoría para archivos, directorios, impresoras y controladores de dominio?
    Si ( ) No (X)

"CUESTIONARIO DE ADMINISTRACIÓN DE LA SEGURIDAD"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Existe una función de investigación dedicada a la evaluación de software, métodos y procedimientos sugeridos en el mercado para la implantación de acciones relativas a la seguridad que brinden un cuidado a los recursos relacionados con la informática?
   Si (X) No ( )
2. ¿Existe administración formal de la red?
   Si (X) No ( )
3. ¿En caso de no tener una administración formal de la red, ¿Se da el seguimiento a los siguientes aspectos?

	Si	*No*
a) Planeación de nueva tecnología de la información (hardware y software)	( )	( )
b) Monitoreo de las actividades de la operación y mantenimiento de la red	( )	( )
c) Procedimientos y control de seguridad	( )	( )
d) Aspectos legales del software instalado	( )	( )
e) Capacitación y soporte a usuarios	( )	( )

4. ¿Existe alguna persona externa que intervenga en la administración de la red?
   Si ( ) No (X)
5. ¿Existe la documentación formal que especifique qué hacer y cómo efectuar las funciones administrativas de la red?
   Si ( ) No (X)
6. ¿Se elaboran políticas y procedimientos de seguridad referente a datos, aplicaciones, hardware, software y accesorios de la red?
   Si ( ) No (X)
7. ¿Cómo se canalizan las dudas, sugerencias y compromisos entre usuarios y responsables de la red? persona a persona
8. ¿Existe una persona encargada de administrar la red?
   Si (X) No ( )
9. ¿Se tiene un control en cuanto al número de horas en las que los usuarios inicien sesiones en la red? Si ( ) No (X)
10. ¿Existen estrategias de organización para usuarios o grupos de usuarios?
    Si ( ) No (X)
11. ¿Se tiene implementado algún plan de cuentas para proteger la red?
    Si (X) No ( )
12. ¿En el caso de contar con carpetas compartidas existe una jerarquía en estas?
    Si ( ) No (X)
13. ¿Se controla el acceso a aplicaciones y datos?
    Si ( ) No (X)
14. ¿Se han organizado los recursos de disco a fin de que las carpetas que tengan los mismos requisitos de seguridad se ubiquen dentro de una misma jerarquía?
    Si ( ) No (X)
15. ¿Se ha documentado que usuarios y permisos se tienen para acceder recursos?
    Si ( ) No (X)
16. ¿Se han establecido directivas de seguridad para asignar permisos de impresión?
    Si ( ) No (X)
17. ¿Se han contemplado planes de auditoria para archivos, directorios, impresoras y controladores de dominio?
    Si (X) No ( )

"CUESTIONARIO DE ADMINISTRACIÓN DE LA SEGURIDAD"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Existe una función de investigación dedicada a la evaluación de software, métodos y procedimientos sugeridos en el mercado para la implantación de acciones relativas a la seguridad que brinden un cuidado a los recursos relacionados con la informatica?
   Si ( ) No (✓)
2. ¿Existe administración formal de la red?
   Si ( ) No (✓)
3. ¿En caso de no tener una administración formal de la red, ¿Se da el seguimiento a los siguientes aspectos?

	Si	*No*
a) Planeación de nueva tecnología de la información (hardware y software)	( )	(✓)
b) Monitoreo de las actividades de la operación y mantenimiento de la red	( )	(✓)
c) Procedimientos y control de seguridad	( )	(✓)
d) Aspectos legales del software instalado	(✓)	( )
e) Capacitación y soporte a usuarios	( )	(✓)

4. ¿Existe alguna persona externa que intervenga en la administración de la red?
   Si (✓) No ( )
5. ¿Existe la documentación formal que especifique qué hacer y cómo efectuar las funciones administrativas de la red?
   Si ( ) No (✓)
6. ¿Se elaboran políticas y procedimientos de seguridad referente a datos, aplicaciones, hardware, software y accesorios de la red?
   Si ( ) No (✓)
7. ¿Cómo se canalizan las dudas, sugerencias y compromisos entre usuarios y responsables de la red? _____
   _____
8. ¿Existe una persona encargada de administrar la red?
   Si ( ) No (✓)
9. ¿Se tiene un control en cuanto al número de horas en las que los usuarios inicien sesiones en la red? Si ( ) No (✓)
10. ¿Existen estrategias de organización para usuarios o grupos de usuarios?
    Si ( ) No (✓)
11. ¿Se tiene implementado algún plan de cuentas para proteger la red?
    Si ( ) No (✓)
12. ¿En el caso de contar con carpetas compartidas existe una jerarquía en estas?
    Si ( ) No (✓)
13. ¿Se controla el acceso a aplicaciones y datos?
    Si ( ) No (✓)
14. ¿Se han organizado los recursos de disco a fin de que las carpetas que tengan los mismos requisitos de seguridad se ubiquen dentro de una misma jerarquía?
    Si ( ) No (✓)
15. ¿Se ha documentado que usuarios y permisos se tienen para acceder recursos?
    Si ( ) No (✓)
16. ¿Se han establecido directivas de seguridad para asignar permisos de impresión?
    Si ( ) No (✓)
17. ¿Se han contemplado planes de auditoria para archivos, directorios, impresoras y controladores de dominio?
    Si ( ) No (✓)

"CUESTIONARIO DE ADMINISTRACIÓN DE LA SEGURIDAD"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Existe una función de investigación dedicada a la evaluación de software, métodos y procedimientos sugeridos en el mercado para la implantación de acciones relativas a la seguridad que brinden un cuidado a los recursos relacionados con la informática?
   Si ( ) No (✓)
2. ¿Existe administración formal de la red?
   Si ( ) No (✓)
3. ¿En caso de no tener una administración formal de la red, ¿Se da el seguimiento a los siguientes aspectos?

	Si	*No*
a) Planeacion de nueva tecnologia de la información (hardware y software)	( )	(✓)
b) Monitoreo de las actividades de la operación y mantenimiento de la red	( )	(✓)
c) Procedimientos y control de seguridad	( )	(✓)
d) Aspectos legales del software instalado	( )	(✓)
e) Capacitación y soporte a usuarios	( )	(✓)

4. ¿Existe alguna persona externa que intervenga en la administración de la red?
   Si ( ) No (✓)
5. ¿Existe la documentación formal que especifique qué hacer y cómo efectuar las funciones administrativas de la red?
   Si ( ) No (✓)
6. ¿Se elaboran políticas y procedimientos de seguridad referente a datos, aplicaciones, hardware, software y accesorios de la red?
   Si ( ) No (✓)
7. ¿Cómo se canalizan las dudas, sugerencias y compromisos entre usuarios y responsables de la red? VERBALMENTE
8. ¿Existe una persona encargada de administrar la red?
   Si (✓) No ( )
9. ¿Se tiene un control en cuanto al número de horas en las que los usuarios inicien sesiones en la red? Si ( ) No (✓)
10. ¿Existen estrategias de organización para usuarios o grupos de usuarios?
    Si ( ) No (✓)
11. ¿Se tiene implementado algún plan de cuentas para proteger la red?
    Si ( ) No (✓)
12. En el caso de contar con carpetas compartidas existe una jerarquía en estas?
    Si ( ) No ( )
13. Se controla el acceso a aplicaciones y datos?
    Si ( ) No (✓)
14. Se han organizado los recursos de disco a fin de que las carpetas que tengan los mismos requisitos de seguridad se ubiquen dentro de una misma jerarquía?
    Si ( ) No (✓)
15. Se ha documentado que usuarios y permisos se tienen para acceder recursos?
    Si ( ) No (✓)
16. Se han establecido directivas de seguridad para asignar permisos de impresión?
    Si ( ) No (✓)
17. Se han contemplado planes de auditoria para archivos, directorios, impresoras y controladores de dominio?
    Si ( ) No (✓)

"CUESTIONARIO DE ADMINISTRACIÓN DE LA SEGURIDAD"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Existe una función de investigación dedicada a la evaluación de software, métodos y procedimientos sugeridos en el mercado para la implantación de acciones relativas a la seguridad que brinden un cuidado a los recursos relacionados con la informática?
   Si ( ) No (X)
2. ¿Existe administración formal de la red?
   Si ( ) No (X)
3. ¿En caso de no tener una administración formal de la red, ¿Se da el seguimiento a los siguientes aspectos?

	Si	*No*
a) Planeación de nueva tecnología de la información (hardware y software)	( )	(X)
b) Monitoreo de las actividades de la operación y mantenimiento de la red	( )	(X)
c) Procedimientos y control de seguridad	( )	(X)
d) Aspectos legales del software instalado	( )	(X)
e) Capacitación y soporte a usuarios	( )	(X)

4. ¿Existe alguna persona externa que intervenga en la administración de la red?
   Si ( ) No (X)
5. ¿Existe la documentación formal que especifique qué hacer y cómo efectuar las funciones administrativas de la red?
   Si ( ) No (X)
6. ¿Se elaboran políticas y procedimientos de seguridad referente a datos, aplicaciones, hardware, software y accesorios de la red?
   Si ( ) No (X)
7. ¿Cómo se canalizan las dudas, sugerencias y compromisos entre usuarios y responsables de la red? Se canaliza en forma directa y verbal
8. ¿Existe una persona encargada de administrar la red?
   Si (X) No ( )
9. ¿Se tiene un control en cuanto al número de horas en las que los usuarios inicien sesiones en la red? Si ( ) No (X)
10. ¿Existen estrategias de organización para usuarios o grupos de usuarios?
    Si ( ) No (X)
11. ¿Se tiene implementado algún plan de cuentas para proteger la red?
    Si ( ) No (X)
12. ¿En el caso de contar con carpetas compartidas existe una jerarquía en estas?
    Si ( ) No (X)
13. ¿Se controla el acceso a aplicaciones y datos?
    Si ( ) No (X)
14. ¿Se han organizado los recursos de disco a fin de que las carpetas que tengan los mismos requisitos de seguridad se ubiquen dentro de una misma jerarquía?
    Si ( ) No (X)
15. ¿Se ha documentado que usuarios y permisos se tienen para acceder recursos?
    Si ( ) No (X)
16. ¿Se han establecido directivas de seguridad para asignar permisos de impresión?
    Si ( ) No (X)
17. ¿Se han contemplado planes de auditoría para archivos, directorios, impresoras y controladores de dominio?
    Si (X) No ( )

"CUESTIONARIO DE ADMINISTRACIÓN DE LA SEGURIDAD"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Existe una función de investigación dedicada a la evaluación de software, métodos y procedimientos sugeridos en el mercado para la implantación de acciones relativas a la seguridad que brinden un cuidado a los recursos relacionados con la informática?
   Si ( ) No (✓)
2. ¿Existe administración formal de la red?
   Si (✓) No ( )
3. ¿En caso de no tener una administración formal de la red, ¿Se da el seguimiento a los siguientes aspectos?

	Si	*No*
a) Planeación de nueva tecnología de la información (hardware y software)	( )	(✓)
b) Monitoreo de las actividades de la operación y mantenimiento de la red	( )	(✓)
c) Procedimientos y control de seguridad	( )	(✓)
d) Aspectos legales del software instalado	(✓)	( )
e) Capacitación y soporte a usuarios	( )	(✓)

4. ¿Existe alguna persona externa que intervenga en la administración de la red?
   Si (✓) No ( )
5. ¿Existe la documentación formal que especifique qué hacer y cómo efectuar las funciones administrativas de la red?
   Si ( ) No (✓)
6. ¿Se elaboran políticas y procedimientos de seguridad referente a datos, aplicaciones, hardware, software y accesorios de la red?
   Si ( ) No (✓)
7. ¿Como se canalizan las dudas, sugerencias y compromisos entre usuarios y responsables de la red? No existe
8. ¿Existe una persona encargada de administrar la red?
   Si (✓) No ( )
9. ¿Se tiene un control en cuanto al número de horas en las que los usuarios inicien sesiones en la red? Si ( ) No (✓)
10. ¿Existen estrategias de organización para usuarios o grupos de usuarios?
    Si ( ) No (✓)
11. ¿Se tiene implementado algún plan de cuentas para proteger la red?
    Si ( ) No (✓)
12. ¿En el caso de contar con carpetas compartidas existe una jerarquía en estas?
    Si ( ) No (✓)
13. ¿Se controla el acceso a aplicaciones y datos?
    Si (✓) No ( )
14. ¿Se han organizado los recursos de disco a fin de que las carpetas que tengan los mismos requisitos de seguridad se ubiquen dentro de una misma jerarquía?
    Si ( ) No (✓)
15. ¿Se ha documentado que usuarios y permisos se tienen para acceder recursos?
    Si (✓) No ( )
16. ¿Se han establecido directivas de seguridad para asignar permisos de impresión?
    Si ( ) No (✓)
17. ¿Se han contemplado planes de auditoria para archivos, directorios, impresoras y controladores de dominio?
    Si ( ) No (✓)

"CUESTIONARIO DE ADMINISTRACIÓN DE LA SEGURIDAD"

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Existe una función de investigación dedicada a la evaluación de software, métodos y procedimientos sugeridos en el mercado para la implantación de acciones relativas a la seguridad que brinden un cuidado a los recursos relacionados con la informática?
   Si ( ) No (X)
2. ¿Existe administración formal de la red?
   Si ( ) No (X)
3. ¿En caso de no tener una administración formal de la red, ¿Se da el seguimiento a los siguientes aspectos?

	Si	*No*
a) Planeación de nueva tecnología de la información (hardware y software)	( )	(X)
b) Monitoreo de las actividades de la operación y mantenimiento de la red	( )	(X)
c) Procedimientos y control de seguridad	( )	(X)
d) Aspectos legales del software instalado	(X)	( )
e) Capacitación y soporte a usuarios	( )	(X)

4. ¿Existe alguna persona externa que intervenga en la administración de la red?
   Si (X) No ( )
5. ¿Existe la documentación formal que especifique qué hacer y cómo efectuar las funciones administrativas de la red?
   Si (X) No ( )
6. ¿Se elaboran políticas y procedimientos de seguridad referente a datos, aplicaciones, hardware, software y accesorios de la red?
   Si ( ) No (X)
7. ¿Cómo se canalizan las dudas, sugerencias y compromisos entre usuarios y responsables de la red? De manera informal y directa
8. ¿Existe una persona encargada de administrar la red?
   Si (X) No ( )
9. ¿Se tiene un control en cuanto al número de horas en las que los usuarios inicien sesiones en la red? Si ( ) No (X)
10. ¿Existen estrategias de organización para usuarios o grupos de usuarios?
    Si ( ) No (X)
11. ¿Se tiene implementado algún plan de cuentas para proteger la red?
    Si ( ) No (X)
12. ¿En el caso de contar con carpetas compartidas existe una jerarquía en estas?
    Si ( ) No (X)
13. ¿Se controla el acceso a aplicaciones y datos?
    Si ( ) No (X)
14. Se han organizado los recursos de disco a fin de que las carpetas que tengan los mismos requisitos de seguridad se ubiquen dentro de una misma jerarquía?
    Si ( ) No (X)
15. Se ha documentado que usuarios y permisos se tienen para acceder recursos?
    Si ( ) No (X)
16. Se han establecido directivas de seguridad para asignar permisos de impresión?
    Si ( ) No (X)
17. Se han contemplado planes de auditoria para archivos, directorios, impresoras y controladores de dominio?
    Si ( ) No (X)

Analisis del Cuestionario sobre la Verificación de los Planes de Continuidad del Negocio

8 cuestionarios aplicados

RESPUESTAS:

a) Tener al personal totalmente parado
b) Es inconveniente, pero las actividades en el departamento continúan
c) No altera en lo absoluto

a)	b)	c)
	8	

PREGUNTA 2

Cuál es el impacto de la interrupción total en los equipos de cómputo, durante varias semanas?

RESPUESTAS:

a) Critia, no hay fuentes de respaldo
b) Existen facilidades de respaldo externas, pero origina mayores costos

a)	b)
	8

PREGUNTA 3

Cuál es la aptitud del personal ante una situación de emergencia?

RESPUESTAS:

a) Se organizan
b) Se organizan a medias
c) Son desorganizados

a)	b)	c)
6	2	

PREGUNTA 4

La localización de sistemas se encuentra en:

RESPUESTAS:

a) Un área especifica
b) En dos o mas áreas
c) Se encuentran en todo el departamento

a)	b)	c)
3	1	4

PREGUNTA 5

Cuál es el tiempo que tarda en recuperarse despés de una interrupción, sea esta cortes de energía eléctrica momentáneos o caída del sistema?

RESPUESTAS:

a) 3 o 4 dias vuelve a la normalidad
b) En 12 o 24 dias
c) La recuperación es casi inmediata

a)	b)	c)
		8

PREGUNTA 6

Como es el control después de una interrupción?

RESPUESTAS:

a) El dano es controlado de forma rápida
b) Es muy dificil de recuperar
c) Es posible mediante copias manuales

a)	b)	c)
6	1	1

"CUESTIONARIO PARA VERIFICAR LOS PLANES DE CONTINUIDAD DEL NEGOCIO".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) **Operaciones fundamentales.**

1. ¿Cuál es el impacto de una hora de interrupción en los equipos de su área de trabajo?
   a) Tener al personal totalmente parado ( )
   b) Es inconveniente, pero las actividades en el departamento continuan (X)
   c) No altera en lo absoluto ( )
2. ¿Cuál es el impacto de la interrupción total en los equipos de cómputo, durante varias semanas?
   a) Critica, no hay fuentes de respaldo (X)
   b) Existen facilidades de respaldo externas, pero origina mayores costos ( )
3. ¿Cuál es la aptitud del personal ante una situación de emergencia?
   a) Se organizan ( )
   b) Se organizan a medias (X)
   c) Son desorganizados ( )
4. La localización de sistemas se encuentra en:
   a) Un área especifica (X)
   b) En dos o más áreas ( )
   c) Se encuentran en todo el departamento ( )
5. ¿Cuál es el tiempo que tarda en reanudarse después de una interrupción, de cortes de energía eléctrica o caída del sistema?
   a) 3 o 4 días vuelve a la normalidad ( )
   b) En 12 o 24 días ( )
   c) La recuperacion es casi inmediata (X)
6. ¿Cómo es el control después de una interrupción?
   a) El daño es controlado de forma rápida ( )
   b) Es muy difícil de recuperar ( )
   c) Es posible mediante copias manuales (X)

"CUESTIONARIO PARA VERIFICAR LOS PLANES DE CONTINUIDAD DEL NEGOCIO".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Operaciones fundamentales.

1. ¿Cuál es el impacto de una hora de interrupción en los equipos de su área de trabajo?
   a) Tener al personal totalmente parado ( )
   b) Es inconveniente, pero las actividades en el departamento continuan (X)
   c) No altera en lo absoluto ( )
2. ¿Cuál es el impacto de la interrupción total en los equipos de cómputo, durante varias semanas?
   a) Critica, no hay fuentes de respaldo (X)
   b) Existen facilidades de respaldo externas, pero origina mayores costos ( )
3. ¿Cuál es la aptitud del personal ante una situación de emergencia?
   a) Se organizan ( )
   b) Se organizan a medias (X)
   c) Son desorganizados ( )
4. La localización de sistemas se encuentra en:
   a) Un área especifica ( )
   b) En dos o más áreas ( )
   c) Se encuentran en todo el departamento (X)
5. ¿Cuál es el tiempo que tarda en reanudarse después de una interrupción, de cortes de energía eléctrica o caida del sistema?
   a) 3 o 4 días vuelve a la normalidad ( )
   b) En 12 o 24 dias ( )
   c) La recuperación es casi inmediata (X)
6. ¿Cómo es el control despues de una interrupción?
   a) El daño es controlado de forma rápida ( )
   b) Es muy difícil de recuperar (X)
   c) Es posible mediante copias manuales ( )

"CUESTIONARIO PARA VERIFICAR LOS PLANES DE CONTINUIDAD DEL NEGOCIO".

Instrucciones: Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).

A) Operaciones **fundamentales.**

1. ¿Cuál es el impacto de una hora de interrupción en los equipos de su área de trabajo?
   a) Tener al personal totalmente parado ( )
   b) Es inconveniente, pero las actividades en el departamento continuan (✓
   c) No altera en lo absoluto ( )
2. ¿Cuál es el impacto de la interrupción total en los equipos de cómputo, durante varias semanas?
   a) Critica, no hay fuentes de respaldo (✓
   b) Existen facilidades de respaldo externas, pero origina mayores costos ( )
3. ¿Cuál es la aptitud del personal ante una situación de emergencia?
   a) Se organizan (✓
   b) Se organizan a medias ( )
   c) Son desorganizados ( )
4. La localización de sistemas se encuentra en:
   a) Un área especifica ( )
   b) En dos o más áreas ( )
   c) Se encuentran en todo el departamento (✓
5. ¿Cuál es el tiempo que tarda en reanudarse después de una interrupción, de cortes de energía eléctrica o caída del sistema?
   a) 3 o 4 días vuelve a la normalidad ( )
   b) En 12 o 24 días ( )
   c) La recuperación es casi inmediata (✓
6. ¿Como es el control después de una interrupción?
   a) El daño es controlado de forma rápida (✓
   b) Es muy difícil de recuperar ( )
   c) Es posible mediante copias manuales ( )

"CUESTIONARIO PARA VERIFICAR LOS PLANES DE CONTINUIDAD DEL NEGOCIO".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) **Operaciones fundamentales.**

1. ¿Cuál es el impacto de una hora de interrupción en los equipos de su área de trabajo?
   a) Tener al personal totalmente parado ( )
   b) Es inconveniente, pero las actividades en el departamento continuan (✓)
   c) No altera en lo absoluto ( )
2. ¿Cuál es el impacto de la interrupción total en los equipos de cómputo, durante varias semanas?
   a) Critica, no hay fuentes de respaldo (✓)
   b) Existen facilidades de respaldo externas, pero origina mayores costos ( )
3. ¿Cuál es la aptitud del personal ante una situación de emergencia?
   a) Se organizan (✓)
   b) Se organizan a medias ( )
   c) Son desorganizados ( )
4. La localización de sistemas se encuentra en:
   a) Un área especifica ( )
   b) En dos o más áreas ( )
   c) Se encuentran en todo el departamento (✓)
5. ¿Cuál es el tiempo que tarda en reanudarse después de una interrupción, de cortes de energía eléctrica o caída del sistema?
   a) 3 o 4 días vuelve a la normalidad ( )
   b) En 12 o 24 días ( )
   c) La recuperación es casi inmediata (✓)
6. ¿Cómo es el control después de una interrupción?
   a) El daño es controlado de forma rápida (✓)
   b) Es muy difícil de recuperar ( )
   c) Es posible mediante copias manuales ( )

"CUESTIONARIO PARA VERIFICAR LOS PLANES DE CONTINUIDAD DEL NEGOCIO".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Operaciones fundamentales.

1. ¿Cuál es el impacto de una hora de interrupción en los equipos de su área de trabajo?
   a) Tener al personal totalmente parado ( )
   b) Es inconveniente, pero las actividades en el departamento continuan (X)
   c) No altera en lo absoluto ( )
2. ¿Cuál es el impacto de la interrupción total en los equipos de cómputo, durante varias semanas?
   a) Critica, no hay fuentes de respaldo (X)
   b) Existen facilidades de respaldo externas, pero origina mayores costos ( )
3. ¿Cuál es la aptitud del personal ante una situación de emergencia?
   a) Se organizan (X)
   b) Se organizan a medias ( )
   c) Son desorganizados ( )
4. La localización de sistemas se encuentra en:
   a) Un área especifica (X)
   b) En dos o más áreas ( )
   c) Se encuentran en todo el departamento ( )
5. ¿Cuál es el tiempo que tarda en reanudarse después de una interrupción, de cortes de energía eléctrica o caida del sistema?
   a) 3 o 4 días vuelve a la normalidad ( )
   b) En 12 o 24 días ( )
   c) La recuperación es casi inmediata (X)
6. ¿Cómo es el control después de una interrupción?
   a) El daño es controlado de forma rápida (X)
   b) Es muy difícil de recuperar ( )
   c) Es posible mediante copias manuales ( )

"CUESTIONARIO PARA VERIFICAR LOS PLANES DE CONTINUIDAD DEL NEGOCIO".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Operaciones fundamentales.

1. ¿Cuál es el impacto de una hora de interrupción en los equipos de su área de trabajo?
   a) Tener al personal totalmente parado ( )
   b) Es inconveniente, pero las actividades en el departamento continuan (X)
   c) No altera en lo absoluto ( )
2. ¿Cuál es el impacto de la interrupción total en los equipos de cómputo, durante varias semanas?
   a) Critica, no hay fuentes de respaldo (X)
   b) Existen facilidades de respaldo externas, pero origina mayores costos ( )
3. ¿Cuál es la aptitud del personal ante una situación de emergencia?
   a) Se organizan (X)
   b) Se organizan a medias ( )
   c) Son desorganizados ( )
4. La localización de sistemas se encuentra en:
   a) Un área especifica ( )
   b) En dos o más áreas ( )
   c) Se encuentran en todo el departamento (X)
5. ¿Cuál es el tiempo que tarda en reanudarse después de una interrupcion, de cortes de energia eléctrica o caida del sistema?
   a) 3 o 4 días vuelve a la normalidad ( )
   b) En 12 o 24 días ( )
   c) La recuperacion es casi inmediata (X)
6. ¿Como es el control de daños de una interrupcion?
   a) El daño es controlado de forma rapida (X)
   b) Es muy difícil de recuperar ( )
   c) Es posible mediante copias manuales ( )

"CUESTIONARIO PARA VERIFICAR LOS PLANES DE CONTINUIDAD DEL NEGOCIO".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

A) Operaciones fundamentales.

1. ¿Cuál es el impacto de una hora de interrupción en los equipos de su área de trabajo?
   a) Tener al personal totalmente parado ( )
   b) Es inconveniente, pero las actividades en el departamento continuan (✓)
   c) No altera en lo absoluto ( )
2. ¿Cuál es el impacto de la interrupción total en los equipos de cómputo, durante varias semanas?
   a) Critica, no hay fuentes de respaldo (✓)
   b) Existen facilidades de respaldo externas, pero origina mayores costos ( )
3. ¿Cuál es la aptitud del personal ante una situación de emergencia?
   a) Se organizan (✓)
   b) Se organizan a medias ( )
   c) Son desorganizados ( )
4. La localización de sistemas se encuentra en:
   a) Un área especifica ( )
   b) En dos o más áreas (✓)
   c) Se encuentran en todo el departamento ( )
5. ¿Cuál es el tiempo que tarda en reanudarse después de una interrupción, de cortes de energía eléctrica o caida del sistema?
   a) 3 o 4 días vuelve a la normalidad ( )
   b) En 12 o 24 días ( )
   c) La recuperación es casi inmediata (✓)
6. ¿Cómo es el control despues de una interrupción?
   a) El daño es controlado de forma rápida (✓)
   b) Es muy difícil de recuperar ( )
   c) Es posible mediante copias manuales ( )

"CUESTIONARIO PARA VERIFICAR LOS PLANES DE CONTINUIDAD DEL NEGOCIO".

Instrucciones: Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).

A) Operaciones **fundamentales.**

1. ¿Cuál es el impacto de una hora de interrupción en los equipos de su área de trabajo?
   a) Tener al personal totalmente parado ( )
   b) Es inconveniente, pero las actividades en el departamento continuan (✓)
   c) No altera en lo absoluto ( )
2. ¿Cuál es el impacto de la interrupción total en los equipos de cómputo, durante varias semanas?
   a) Critica, no hay fuentes de respaldo (✓)
   b) Existen facilidades de respaldo externas, pero origina mayores costos ( )
3. ¿Cuál es la aptitud del personal ante una situación de emergencia?
   a) Se organizan (✓)
   b) Se organizan a medias ( )
   c) Son desorganizados ( )
4. La localización de sistemas se encuentra en:
   a) Un área especifica (✓)
   b) En dos o más áreas ( )
   c) Se encuentran en todo el departamento ( )
5. ¿Cual es el tiempo que tarda en reanudarse después de una interrupción, de cortes de energía electrica o caida del sistema?
   a) 3 o 4 días vuelve a la normalidad ( )
   b) En 12 o 24 días ( )
   c) La recuperación es casi inmediata (✓)
6. ¿Como es el control despues de una interrupción?
   a) El daño es controlado de forma rapida (✓)
   b) Es muy difícil de recuperar ( )
   c) Es posible mediante copias manuales ( )

Analisis del Cuestionario sobre Seguridad en la Red

8 cuestionarios aplicados

PREGUNTA 1

Hay procedimientos que protejan los datos transmitidos en la red, si es así menciónelos?

RESPUESTAS:

Si	No
1	7

la codificación

PREGUNTA 2

Existen registros con información relevante sobre el comportamiento de la red?

RESPUESTAS:

Si	No
2	6

PREGUNTA 3

La red tiene controles de acceso a datos no autorizados?

RESPUESTAS:

Si	No
3	5

PREGUNTA 4

Existen controles relativos a la seguridad física de los diversos componentes de la red como los son tarjetas, terminales, manuales, teclados, ratones, etc?

RESPUESTAS:

Si	No
5	3

PREGUNTA 5

Se tiene un seguro que proteja el sotware y equipo de la red?

RESPUESTAS:

Si	No
2	5

PREGUNTA 6

Se cuenta con alternativas que apoyen al departamento en caso de alguna falla generalizada y prolongada en la red?

RESPUESTAS:

Si	No
3	5

PREGUNTA 7

Se verifica la identificación de terminales y usuarios?

RESPUESTAS:

Si	No
4	4

PREGUNTA 8

Se registra la violación de procedimientos de acceso a las máquinas con el fin de llevar una estadistica y frenar

RESPUESTAS:

Si	No
	8

PREGUNTA 9

Se cuenta con manuales de operación de la red?

RESPUESTAS:

Si	No
1	7

Analisis del Cuestionario sobre Seguridad en la Red

PREGUNTA 10

Fue capacitado y preparado el personal para administrar y operar la red?

RESPUESTAS:

Si	No
1	7

PREGUNTA 11

Se evalúa el desempeño de la red en medida del tiempo de respuesta y recuperación de la misma?

RESPUESTAS:

Si	No
	7

PREGUNTA 12

Se da un mantenimiento a la red, donde se indiquen las fechas y responsables de hacerlo?

RESPUESTAS:

Si	No
1	7

PREGUNTA 13

Se han tomado en cuenta algunas consideraciones complementarias que ayuden al mejoramiento continuo de la red local como las siguientes?

RESPUESTAS:

	Si	No
a) Evaluacion periodica de la red : hardware, software, grado de utilizacion.	1	7
b) Acceso de nuevos usuarios a la red, niveles de perfil de usuario, asignacion de software o datos para utilizar, consultar, borrar, modificar.	3	5
c) Capacitacion, planeacion, ejecucion y actualizacion.		8
d) Crecimiento de la red: perifericos, mamoria, usuarios, aplicaciones.	2	6
e) Respaldo: datos, equipo, perifericos, software, aplicaciones.	3	5
f) Seguridad en el procesamiento, planes de recuperacion		8

PREGUNTA 14

Señale si tiene identificada formalmente la siguiente información:

RESPUESTAS:

	Si	No
usuarios de la red	5	3
Registro y niveles de acceso	2	6
Terminales conectadas a la red	6	2
Responsables de la red	6	2
Procedimientos de contingencia		8
Software	4	4
Perifericos conectados	3	5
Software original y pirata instalado	4	4
Tipos de unidades centrales	3	5
Capacidad de disco	4	4

"CUESTIONARIO DE SEGURIDAD EN LA RED".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Hay procedimientos que protejan los datos transmitidos en la red, si es así menciónelos?
   Si ( ) No (X)
2. ¿Existen registros con información relevante sobre el comportamiento de la red?
   Si (X) No ( )
3. ¿La red tiene controles de acceso a datos no autorizados?
   Si ( ) No (X)
4. ¿Existen controles relativos a la seguridad física de los diversos componentes de la red como lo son tarjetas, terminales, manuales, teclados, ratones, etc?
   Si (X) No ( )
5. ¿Se tiene un seguro que proteja el software y equipo de red?
   Si ( ) No (X)
6. ¿Se cuenta con alternativas que apoyen al Departamento en caso de alguna falla generalizada y prolongada en la red?
   Si ( ) No (X)
7. ¿Se verifica la identificación de terminales y usuarios?
   Si ( ) No (X)
8. ¿Se registra la violación de procedimientos de acceso a las máquinas con el fin de llevar una estadística y fronar tendencias?
   Si ( ) No (X)
9. ¿Se cuenta con manuales de operación de la red?
   Si ( ) No (X)
10. ¿Fue capacitado y preparado el personal para administrar y operar la red?
    Si ( ) No (X)
11. ¿Se evalúa el desempeño de la red en medida del tiempo de respuesta y recuperación de la misma?
    Si ( ) No (X)
12. ¿Se da un mantenimiento a la red, donde se indiquen las fechas y responsables para hacerlo?
    Si ( ) No (X)
13. ¿Se han tomado en cuenta algunas consideraciones complementarias que ayuden al mejoramiento continuo de la red local como las siguientes?

	Si	*No*
a) Evaluación periódica de la red: hardware, software, grado de utilización.	( )	(X)
b) Acceso de nuevos usuarios a la red, niveles de perfil de usuario, asignación de software o datos para utilizar, consultar, borrar, modificar.	(X)	( )
c) Capacitación, planeación, ejecución y actualización.	( )	(X)
d) Crecimiento de la red: periféricos, memoria, usuarios, aplicaciones	(X)	( )
e) Respaldo: datos, equipo, periféricos, software, aplicaciones.	(X)	( )
f) Seguridad en el procesamiento, planes de recuperación.	( )	(X)

14. Señale si tiene identificada formalmente la siguiente información:

	Si	*No*
a) Usuarios de la red	(X)	( )
b) Registro y niveles de acceso.	( )	(X)
c) Terminales conectadas a la red	(X)	( )
d) Responsables de la red	(X)	( )
e) Procedimientos de contingencia	( )	(X)
f) Software	(X)	( )
g) Periféricos conectados	( )	(X)
h) Software original y pirata instalado	(X)	( )
i)Tipos de unidades centrales de procesamiento	( )	(X)
j) Capacidad de disco o espacio libre en el servidor	(X)	( )

"CUESTIONARIO DE SEGURIDAD EN LA RED".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Hay procedimientos que protejan los datos transmitidos en la red, si es así menciónelos?
   Si ( ) No (X)
2. ¿Existen registros con información relevante sobre el comportamiento de la red?
   Si ( ) No (X)
3. ¿La red tiene controles de acceso a datos no autorizados?
   Si ( ) No (X)
4. ¿Existen controles relativos a la seguridad física de los diversos componentes de la red como lo son tarjetas, terminales, manuales, teclados, ratones, etc?
   Si ( ) No (X)
5. ¿Se tiene un seguro que proteja el software y equipo de red?
   Si ( ) No (X)
6. ¿Se cuenta con alternativas que apoyen al Departamento en caso de alguna falla generalizada y prolongada en la red?
   Si (X) No ( )
7. ¿Se verifica la identificación de terminales y usuarios?
   Si (X) No ( )
8. ¿Se registra la violación de procedimientos de acceso a las máquinas con el fin de llevar una estadística y frenar tendencias?
   Si ( ) No (X)
9. ¿Se cuenta con manuales de operación de la red?
   Si ( ) No (X)
10. ¿Fue capacitado y preparado el personal para administrar y operar la red?
    Si ( ) No (X)
11. ¿Se evalúa el desempeño de la red en medida del tiempo de respuesta y recuperación de la misma?
    Si ( ) No (X)
12. ¿Se da un mantenimiento a la red, donde se indiquen las fechas y responsables para hacerlo?
    Si ( ) No (X)
13. ¿Se han tomado en cuenta algunas consideraciones complementarias que ayuden al mejoramiento continuo de la red local como las siguientes?

	Si	*No*
a) Evaluación periódica de la red: hardware, software, grado de utilización.	( )	(X)
b) Acceso de nuevos usuarios a la red, niveles de perfil de usuario, asignación de software o datos para utilizar, consultar, borrar, modificar.	( )	(X)
c) Capacitación, planeación, ejecución y actualización.	( )	(X)
d) Crecimiento de la red: periféricos, memoria, usuarios, aplicaciones	( )	(X)
e) Respaldo: datos, equipo, periféricos, software, aplicaciones.	( )	(X)
f) Seguridad en el procesamiento, planes de recuperación.	( )	(X)

14. Señale si tiene identificada formalmente la siguiente información:

	Si	*No*
a) Usuarios de la red	( )	(X)
b) Registro y niveles de acceso.	( )	(X)
c) Terminales conectadas a la red	(X)	( )
d) Responsables de la red	(X)	( )
e) Procedimientos de contingencia	( )	(X)
f) Software	(X)	( )
g) Periféricos conectados	(X)	( )
h) Software original y pirata instalado	(X)	( )
i) Tipos de unidades centrales de procesamiento	(X)	( )
j) Capacidad de disco o espacio libre en el servidor	(X)	( )

"CUESTIONARIO DE SEGURIDAD EN LA RED".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Hay procedimientos que protejan los datos transmitidos en la red, si es así menciónelos?
   Si ( ) No (✓)
2. ¿Existen registros con información relevante sobre el comportamiento de la red?
   Si ( ) No (✓)
3. ¿La red tiene controles de acceso a datos no autorizados?
   Si ( ) No (✓)
4. ¿Existen controles relativos a la seguridad física de los diversos componentes de la red como lo son tarjetas, terminales, manuales, teclados, ratones, etc?
   Si (✓) No ( )
5. ¿Se tiene un seguro que proteja el software y equipo de red?
   Si (✓) No ( )
6. ¿Se cuenta con alternativas que apoyen al Departamento en caso de alguna falla generalizada y prolongada en la red?
   Si (✓) No ( )
7. ¿Se verifica la identificación de terminales y usuarios?
   Si ( ) No (✓)
8. ¿Se registra la violación de procedimientos de acceso a las máquinas con el fin de llevar una estadística y frenar tendencias?
   Si ( ) No (✓)
9. ¿Se cuenta con manuales de operación de la red?
   Si ( ) No (✓)
10. ¿Fue capacitado y preparado el personal para administrar y operar la red?
    Si ( ) No (✓)
11. ¿Se evalúa el desempeño de la red en medida del tiempo de respuesta y recuperación de la misma?
    Si ( ) No (✓)
12. ¿Se da un mantenimiento a la red, donde se indiquen las fechas y responsables para hacerlo?
    Si ( ) No (✓)
13. ¿Se han tomado en cuenta algunas consideraciones complementarias que ayuden al mejoramiento continuo de la red local como las siguientes?

	Si	*No*
a) Evaluación periódica de la red: hardware, software, grado de utilización.	( )	(✓)
b) Acceso de nuevos usuarios a la red, niveles de perfil de usuario, asignación de software o datos para utilizar, consultar, borrar, modificar.	( )	(✓)
c) Capacitacion, planeación, ejecución y actualización.	( )	(✓)
d) Crecimiento de la red: periféricos, memoria, usuarios, aplicaciones	( )	(✓)
e) Respaldo: datos, equipo, periféricos, software, aplicaciones.	( )	(✓)
f) Seguridad en el procesamiento, planes de recuperación.	( )	(✓)

14. Señale si tiene identificada formalmente la siguiente información:

	Si	*No*
a) Usuarios de la red	( )	(✓)
b) Registro y niveles de acceso.	( )	(✓)
c) Terminales conectadas a la red	( )	(✓)
d) Responsables de la red	(✓)	( )
e) Procedimientos de contingencia	( )	(✓)
f) Software	( )	(✓)
g) Periféricos conectados	( )	(✓)
h) Software original y pirata instalado	( )	(✓)
i) Tipos de unidades centrales de procesamiento	( )	(✓)
j) Capacidad de disco o espacio libre en el servidor	( )	(✓)

"CUESTIONARIO DE SEGURIDAD EN LA RED".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Hay procedimientos que protejan los datos transmitidos en la red, si es así menciónelos?
   Si ( ) No (X)
2. ¿Existen registros con información relevante sobre el comportamiento de la red?
   Si ( ) No (X)
3. ¿La red tiene controles de acceso a datos no autorizados?
   Si ( ) No (X)
4. ¿Existen controles relativos a la seguridad física de los diversos componentes de la red como lo son tarjetas, terminales, manuales, teclados, ratones, etc?
   Si (X) No ( )
5. ¿Se tiene un seguro que proteja el software y equipo de red?
   Si (X) No ( )
6. ¿Se cuenta con alternativas que apoyen al Departamento en caso de alguna falla generalizada y prolongada en la red?
   Si ( ) No (X)
7. ¿Se verifica la identificación de terminales y usuarios?
   Si (X) No ( )
8. ¿Se registra la violación de procedimientos de acceso a las máquinas con el fin de llevar una estadística y frenar tendencias?
   Si ( ) No (X)
9. ¿Se cuenta con manuales de operación de la red?
   Si ( ) No (X)
10. ¿Fue capacitado y preparado el personal para administrar y operar la red?
    Si ( ) No (X)
11. ¿Se evalúa el desempeño de la red en medida del tiempo de respuesta y recuperación de la misma?
    Si ( ) No (X)
12. ¿Se da un mantenimiento a la red, donde se indiquen las fechas y responsables para hacerlo?
    Si ( ) No (X)
13. ¿Se han tomado en cuenta algunas consideraciones complementarias que ayuden al mejoramiento continuo de la red local como las siguientes?

	Si	*No*
a) Evaluación periódica de la red: hardware, software, grado de utilización.	( )	(X)
b) Acceso de nuevos usuarios a la red, niveles de perfil de usuario, asignación de software o datos para utilizar, consultar, borrar, modificar.	( )	(X)
c) Capacitación, planeación, ejecución y actualización.	( )	(X)
d) Crecimiento de la red: periféricos, memoria, usuarios, aplicaciones	( )	(X)
e) Respaldo: datos, equipo, periféricos, software, aplicaciones.	( )	(X)
f) Seguridad en el procesamiento, planes de recuperación.	( )	(X)

14. Señale si tiene identificada formalmente la siguiente información:

	Si	*No*
a) Usuarios de la red	(X)	( )
b) Registro y niveles de acceso.	( )	(X)
c) Terminales conectadas a la red	(X)	( )
d) Responsables de la red	(X)	( )
e) Procedimientos de contingencia	( )	(X)
f) Software	(X)	( )
g) Periféricos conectados	(X)	( )
h) Software original y pirata instalado	(X)	( )
i) Tipos de unidades centrales de procesamiento	(X)	( )
j) Capacidad de disco o espacio libre en el servidor	( )	(X)

"CUESTIONARIO DE SEGURIDAD EN LA RED".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Hay procedimientos que protejan los datos transmitidos en la red, si es así menciónelos?
   Si ( ) No (✓)
2. ¿Existen registros con información relevante sobre el comportamiento de la red?
   Si ( ) No (✓)
3. ¿La red tiene controles de acceso a datos no autorizados?
   Si ( ) No (✓)
4. ¿Existen controles relativos a la seguridad física de los diversos componentes de la red como lo son tarjetas, terminales, manuales, teclados, ratones, etc?
   Si ( ) No (✓)
5. ¿Se tiene un seguro que proteja el software y equipo de red?
   Si ( ) No (✓)
6. ¿Se cuenta con alternativas que apoyen al Departamento en caso de alguna falla generalizada y prolongada en la red?
   Si ( ) No (✓)
7. ¿Se verifica la identificación de terminales y usuarios?
   Si ( ) No (✓)
8. ¿Se registra la violación de procedimientos de acceso a las máquinas con el fin de llevar una estadística y frenar tendencias?
   Si ( ) No (✓)
9. ¿Se cuenta con manuales de operación de la red?
   Si ( ) No (✓)
10. ¿Fue capacitado y preparado el personal para administrar y operar la red?
    Si ( ) No (✓)
11. ¿Se evalúa el desempeño de la red en medida del tiempo de respuesta y recuperación de la misma?
    Si ( ) No (✓)
12. ¿Se da un mantenimiento a la red, donde se marquen las fechas y responsables para hacerlo?
    Si ( ) No (✓)
13. ¿Se han tomado en cuenta algunas consideraciones complementarias que ayuden al mejoramiento continuo de la red local como las siguientes?

	Si	*No*
a) Evaluación periódica de la red: hardware, software, grado de utilización.	( )	(✓)
b) Acceso de nuevos usuarios a la red, niveles de perfil de usuario, asignación de software o datos para utilizar, consultar, borrar, modificar.	( )	(✓)
c) Capacitación, planeación, ejecución y actualización.	( )	(✓)
d) Crecimiento de la red: periféricos, memoria, usuarios, aplicaciones	(✓)	(✓)
e) Respaldo: datos, equipo, periféricos, software, aplicaciones.	(✓)	( )
f) Seguridad en el procesamiento, planes de recuperación.	( )	(✓)

14. Señale si tiene identificada formalmente la siguiente información:

	Si	*No*
a) Usuarios de la red	( )	(✓)
b) Registro y niveles de acceso.	(✓)	( )
c) Terminales conectadas a la red	(✓)	( )
d) Responsables de la red	(✓)	( )
e) Procedimientos de contingencia	( )	(✓)
f) Software	( )	(✓)
g) Periféricos conectados	( )	(✓)
h) Software original y pirata instalado	( )	(✓)
i) Tipos de unidades centrales de procesamiento	( )	(✓)
j) Capacidad de disco o espacio libre en el servidor	( )	(✓)

"CUESTIONARIO DE SEGURIDAD EN LA RED".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Hay procedimientos que protejan los datos transmitidos en la red, si es así menciónelos?
   Si (✓) No ( )
2. ¿Existen registros con información relevante sobre el comportamiento de la red?
   Si (✓) No ( )
3. ¿La red tiene controles de acceso a datos no autorizados?
   Si (✓) No ( )
4. ¿Existen controles relativos a la seguridad física de los diversos componentes de la red como lo son tarjetas, terminales, manuales, teclados, ratones, etc?
   Si (✓) No ( )
5. ¿Se tiene un seguro que proteja el software y equipo de red?
   Si ( ) No (✓)
6. ¿Se cuenta con alternativas que apoyen al Departamento en caso de alguna falla generalizada y prolongada en la red?
   Si ( ) No (✓)
7. ¿Se verifica la identificación de terminales y usuarios?
   Si (✓) No ( )
8. ¿Se registra la violación de procedimientos de acceso a las máquinas con el fin de llevar una estadística y frenar tendencias?
   Si ( ) No (✓)
9. ¿Se cuenta con manuales de operación de la red?
   Si (✓) No ( )
10. ¿Fue capacitado y preparado el personal para administrar y operar la red?
    Si (✓) No ( )
11. ¿Se evalúa el desempeño de la red en medida del tiempo de respuesta y recuperación de la misma?
    Si ( ) No (✓)
12. ¿Se da un mantenimiento a la red, donde se indiquen las fechas y responsables para hacerlo?
    Si ( ) No (✓)
13. ¿Se han tomado en cuenta algunas consideraciones complementarias que ayuden al mejoramiento continuo de la red local como las siguientes?

	Si	*No*
a) Evaluación periódica de la red: hardware, software, grado de utilización.	( )	(✓)
b) Acceso de nuevos usuarios a la red, niveles de perfil de usuario, asignación de software o datos para utilizar, consultar, borrar, modificar.	(✓)	( )
c) Capacitación, planeación, ejecución y actualización.	( )	(✓)
d) Crecimiento de la red: periféricos, memoria, usuarios, aplicaciones	( )	(✓)
e) Respaldo: datos, equipo, periféricos, software, aplicaciones.	( )	(✓)
f) Seguridad en el procesamiento, planes de recuperación.	( )	(✓)

14. Señale si tiene identificada formalmente la siguiente información:

	Si	*No*
a) Usuarios de la red	(✓)	( )
b) Registro y niveles de acceso.	(✓)	( )
c) Terminales conectadas a la red	(✓)	( )
d) Responsables de la red	(✓)	( )
e) Procedimientos de contingencia	( )	(✓)
f) Software	(✓)	( )
g) Periféricos conectados	(✓)	( )
h) Software original y pirata instalado	(✓)	( )
i) Tipos de unidades centrales de procesamiento	(✓)	( )
j) Capacidad de disco o espacio libre en el servidor	(✓)	( )

"CUESTIONARIO DE SEGURIDAD EN LA RED".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Hay procedimientos que protejan los datos transmitidos en la red, si es así menciónelos?
   Si ( ) No (X)
2. ¿Existen registros con información relevante sobre el comportamiento de la red?
   Si ( ) No (X)
3. ¿La red tiene controles de acceso a datos no autorizados?
   Si (X) No ( )
4. ¿Existen controles relativos a la seguridad física de los diversos componentes de la red como lo son tarjetas, terminales, manuales, teclados, ratones, etc?
   Si ( ) No (X)
5. ¿Se tiene un seguro que proteja el software y equipo de red?
   Si ( ) No (X)
6. ¿Se cuenta con alternativas que apoyen al Departamento en caso de alguna falla generalizada y prolongada en la red?
   Si (X) No ( )
7. ¿Se verifica la identificación de terminales y usuarios?
   Si (X) No ( )
8. ¿Se registra la violación de procedimientos de acceso a las máquinas con el fin de llevar una estadística y frenar tendencias?
   Si ( ) No (X)
9. ¿Se cuenta con manuales de operación de la red?
   Si ( ) No (X)
10. ¿Fue capacitado y preparado el personal para administrar y operar la red?
    Si ( ) No (X)
11. ¿Se evalúa el desempeño de la red en medida del tiempo de respuesta y recuperación de la misma?
    Si ( ) No (X)
12. ¿Se da un mantenimiento a la red, donde se indiquen las fechas y responsables para hacerlo?
    Si (X) No ( )
13. ¿Se han tomado en cuenta algunas consideraciones complementarias que ayuden al mejoramiento continuo de la red local como las siguientes?

	Si	No
a) Evaluación periódica de la red: hardware, software, grado de utilización.	(X)	( )
b) Acceso de nuevos usuarios a la red, niveles de perfil de usuario, asignación de software o datos para utilizar, consultar, borrar, modificar.	(X)	( )
c) Capacitación, planeación, ejecución y actualización.	( )	(X)
d) Crecimiento de la red: periféricos, memoria, usuarios, aplicaciones	(X)	( )
e) Respaldo: datos, equipo, periféricos, software, aplicaciones.	(X)	( )
f) Seguridad en el procesamiento, planes de recuperación.	( )	(X)

14. Señale si tiene identificada formalmente la siguiente información:

	Si	No
a) Usuarios de la red	(X)	( )
b) Registro y niveles de acceso.	(X)	( )
c) Terminales conectadas a la red	(X)	( )
d) Responsables de la red	( )	(X)
e) Procedimientos de contingencia	( )	(X)
f) Software	(X)	( )
g) Periféricos conectados	( )	(X)
h) Software original y pirata instalado	( )	(X)
i) Tipos de unidades centrales de procesamiento	( )	(X)
j) Capacidad de disco o espacio libre en el servidor	( )	(X)

"CUESTIONARIO DE SEGURIDAD EN LA RED".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1. ¿Hay procedimientos que protejan los datos transmitidos en la red, si es así menciónelos?
   Si ( ) No (X)
2. ¿Existen registros con información relevante sobre el comportamiento de la red?
   Si ( ) No (X)
3. ¿La red tiene controles de acceso a datos no autorizados?
   Si (X) No ( )
4. ¿Existen controles relativos a la seguridad física de los diversos componentes de la red como lo son tarjetas, terminales, manuales, teclados, ratones, etc?
   Si (X) No ( )
5. ¿Se tiene un seguro que proteja el software y equipo de red?
   Si ( ) No (X)
6. ¿Se cuenta con alternativas que apoyen al Departamento en caso de alguna falla generalizada y prolongada en la red?
   Si ( ) No (X)
7. ¿Se verifica la identificación de terminales y usuarios?
   Si ( ) No (X)
8. ¿Se registra la violación de procedimientos de acceso a las máquinas con el fin de llevar una estadística y frenar tendencias?
   Si ( ) No (X)
9. ¿Se cuenta con manuales de operación de la red?
   Si ( ) No (X)
10. ¿Fue capacitado y preparado el personal para administrar y operar la red?
    Si ( ) No (X)
11. ¿Se evalúa el desempeño de la red en medida del tiempo de respuesta y recuperación de la misma?
    Si ( ) No (X)
12. ¿Se da un mantenimiento a la red, donde se indiquen las fechas y responsables para hacerlo?
    Si ( ) No (X)
13. ¿Se han tomado en cuenta algunas consideraciones complementarias que ayuden al mejoramiento continuo de la red local como las siguientes?

	Si	No
a) Evaluación periódica de la red: hardware, software, grado de utilización.	( )	(X)
b) Acceso de nuevos usuarios a la red, niveles de perfil de usuario, asignación de software o datos para utilizar, consultar, borrar, modificar.	( )	(X)
c) Capacitación, planeación, ejecución y actualización.	( )	(X)
d) Crecimiento de la red: periféricos, memoria, usuarios, aplicaciones	( )	(X)
e) Respaldo: datos, equipo, periféricos, software, aplicaciones.	( )	(X)
f) Seguridad en el procesamiento, planes de recuperación.	( )	(X)

14. Señale si tiene identificada formalmente la siguiente información:

	Si	No
a) Usuarios de la red	(X)	( )
b) Registro y niveles de acceso	( )	(X)
c) Terminales conectadas a la red	(X)	( )
d) Responsables de la red	(X)	( )
e) Procedimientos de contingencia	( )	(X)
f) Software	( )	(X)
g) Periféricos conectados	( )	(X)
h) Software original y pirata instalado	( )	(X)
i) Tipos de unidades centrales de procesamiento	( )	(X)
j) Capacidad de disco o espacio libre en el servidor	(X)	( )

Analisis del Cuestionario sobre Seguridad en Internet

3 cuestionarios aplicados

cuenta su equipó con un antivurus actualizado?

RESPUESTAS:

SI	No
3	

PREGUNTA 2

Qué tipo de navegador de red utiliza?

RESPUESTAS:

Neiscape	
Explorer	
MSN Explorer	3
Otro	

PREGUNTA 3

Se utilizan programas de seguridad para controlar las cookies que envían datos devuelta a los sitios web?

RESPUESTAS

SI	No
3	

PREGUNTA 4

Se garantiza la transferencia segura de información al usuario final?

RESPUESTAS

SI	No
3	

PREGUNTA 5

Se cerciora de obtener información relativa del nivel de seguridad existente en el servidor que hospeda las pa

RESPUESTAS

SI	No
3	

PREGUNTA 6

Al intercambiar información verifica lo siguiente?

RESPUESTAS

	SI	No
El cambio de protocolo http en la ventana de direcciones	3	
Que exista un icono de seguridad (candado o llave de navegador)	1	2

PREGUNTA 7

Se ha fomentado el uso de certificados personales de seguridad para proteger su identidad en internet?

RESPUESTAS

SI	No
2	1

PREGUNTA 8

Cuando usted descarga un archivo generalmente?

RESPUESTAS

Lo abre desde el Origen	2
Lo guarda en disco	1

PREGUNTA 9

Se cuenta con alguno de éstos dispositivos de seguridad?

RESPUESTAS

	Repetidores
3	Concentradores (HUB)
	Puentes (BRIDGES)
	Encaminadores (routers)
	Pasarelas (gateway)

"CUESTIONARIO DE SEGURIDAD EN INTERNET".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1.- ¿Cuenta su equipo con un antivirus actualizado?
Si (X) No ( )

2.- ¿Qué tipo de navegador de red utiliza?
Netscape ( )
Explorer ( )
MSN Explorer (X)
Otro ( ) Menciónelo _____

3.- ¿Se utilizan programas de seguridad para controlar las Cookies que envían datos devuelta a los sitios Web?
Si (X) No ( )

4.- ¿Se garantiza la transferencia segura de información al usuario final?
Si (X) No ( )

5.- ¿Se cerciora de obtener información relativa del nivel de seguridad existente en el servidor que hospeda las páginas que usted?
Si (X) No ( )

6.- ¿Al intercambiar información verifica lo siguiente?

		Si	No
a)	El cambio de protocolo HTTP en la ventana de direcciones	(X)	( )
b)	Que exista un icono de seguridad (candado o llave de navegador)	( )	(X)

7.- ¿Se ha fomentado el uso de certificados personales de seguridad para proteger su identidad en Internet?
Si ( ) No (X)

8.- ¿Que es lo que realiza generalmente cuando descarga un archivo?
a) Lo abre desde el origen (X)
b) Lo guarda en disco ( )

9.- ¿Con qué dispositivos de seguridad se cuenta?
a) Repetidores ( )
b) Concentradores (hub's) (X)
c) Puentes (Bridges) ( )
d) Encaminadotes (routers) ( )
e) Pasarela Gateway) ( )

"CUESTIONARIO DE SEGURIDAD EN INTERNET".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1.- ¿Cuenta su equipo con un antivirus actualizado?
Si (✓) No ( )

2.- ¿Qué tipo de navegador de red utiliza?
Netscape ( )
Explorer ( )
MSN Explorer (✓)
Otro ( ) Menciónelo _____

3.- ¿Se utilizan programas de seguridad para controlar las Cookies que envian datos devuelta a los sitios Web?
Si (✓) No ( )

4.- ¿Se garantiza la transferencia segura de información al usuario final?
Si (✓) No ( )

5.- ¿Se cerciora de obtener información relativa del nivel de seguridad existente en el servidor que hospeda las páginas que usted?
Si (✓) No ( )

6.- ¿Al intercambiar información verifica lo siguiente?

		Si	No
a)	El cambio de protocolo HTTP en la ventana de direcciones	(✓)	( )
b)	Que exista un icono de seguridad (candado o llave de navegador)	(✓)	( )

7.- ¿Se ha fomentado el uso de certificados personales de seguridad para proteger su identidad en Internet?
Si (✓) No ( )

8.- ¿Qué es lo que realiza generalmente cuando descarga un archivo?
a) Lo abre desde el origen ( )
b) Lo guarda en disco (✓)

9.- ¿Con qué dispositivos de seguridad se cuenta?
a) Repetidores ( )
b) Concentradores (hub's) (✓)
c) Puentes (Bridges) ( )
d) Encaminadotes (routers) ( )
e) Pasarela Gateway) ( )

"CUESTIONARIO DE SEGURIDAD EN INTERNET".

Instrucciones: *Marque dentro de los paréntesis la respuesta que considere más conveniente de acuerdo a su experiencia (una sola respuesta).*

1.- ¿Cuenta su equipo con un antivirus actualizado?
Si (X) No ( )

2.- ¿Qué tipo de navegador de red utiliza?
Netscape ( )
Explorer ( )
MSN Explorer (X)
Otro ( ) Menciónelo _____

3.- ¿Se utilizan programas de seguridad para controlar las Cookies que envían datos devuelta a los sitios Web?
Si (X) No ( )

4.- ¿Se garantiza la transferencia segura de información al usuario final?
Si (X) No ( )

5.- ¿Se cerciora de obtener información relativa del nivel de seguridad existente en el servidor que hospeda las páginas que usted?
Si (X) No ( )

6.- ¿Al intercambiar información verifica lo siguiente?

		Si	No
a)	El cambio de protocolo HTTP en la ventana de direcciones	(X)	( )
b)	Que exista un icono de seguridad (candado o llave de navegador)	( )	(X)

7.- ¿Se ha fomentado el uso de certificados personales de seguridad para proteger su identidad en Internet?
Si (X) No ( )

8.- ¿Qué es lo que realiza generalmente cuando descarga un archivo?
a) Lo abre desde el origen (X)
b) Lo guarda en disco ( )

9.- ¿Con qué dispositivos de seguridad se cuenta?
a) Repetidores ( )
b) Concentradores (hub's) (X)
c) Puentes (Bridges) ( )
d) Encaminadores (routers) ( )
e) Pasarela Gateway) ( )

ANEXO 4

Compromiso de Formación del Comité

Formación del Comité de Seguridad, En Informática De Talleres La Paz. (STC).

Con este comité se pretende formar un equipo de trabajo que coordine y auxilie el apoyo informático de los talleres mediante la coordinación de la revisión de manera regular y sorpresiva, así como realizar las acciones correctivas y preventivas apropiadas.

El objetivo principal de éste comité es el de garantizar una seguridad efectiva en los talleres, como lo es también el diseño y aplicación de planes efectivos contra posibles desastres.

No se necesitará mucho tiempo del que usted dispone, ya que son reuniones de forma mensual o cada 6 meses según las necesidades del taller.

Para lograrlo se necesita un representante de cada área de trabajo:

REPRESENTANTE	ÁREA
1.- Nombre y firma	Coordinación de Servicios al Material Rodante.
2.- Nombre y firma	Coordinación de Mantenimiento Menor.
3.- ING. Nombre y firma	Coordinación Electromecánica.
4.- Nombre y firma	Centro de Información de Línea.
5.- Nombre y firma	Ingeniería y Aseguramiento de Calidad.
6.- Nombre y firma	Mantenimiento Mayor.

SUPLENTES

1.-
2.-
3.-
4.-
5.-
6.-

Vo.Bo.

Ing. Gerardo J. Cruz Chacón
Jefe del Departamento de
Servicios de Mantenimiento al Material
Rodante Férreo.