REPÚBLICA DEL ECUADOR

UNIVERSIDAD ESTATAL DE MILAGRO

INSTITUTO DE POSTGRADO Y EDUCACIÓN CONTINUA

PROYECTO DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGÍSTER EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN

TÍTULO DEL PROYECTO:

ANALISIS DE LA AUDITORIA EN SEGURIDAD INFORMATICA DELDEPARTAMENTO DE TECNOLOGIAS DE LA UNEMI.

TUTOR

DR. GUSTAVO H. GALIO MOLINA MSc.

AUTOR

ING. JAVIER RICARDO BERMEO PAUCAR

MILAGRO, 2012

UNIVERSIDAD ESTATAL DE MILAGRO

INSTITUTO DE POSTGRADO Y EDUCACIÓN CONTINUA

EL TRIBUNAL EXAMINADOR OTORGA A ESTE PROYECTO DE INVESTIGACIÓN

LA CALIFICACIÓN DE: _____

EQUIVALENTE A: _____

_____

Nombre:

ASESOR DEL PROYECTO

_____

Nombre:

PRESIDENTE(A) DEL TRIBUNAL

_____

Nombre:

SECRETARIO(A) DEL TRIBUNAL

Milagro, _____de _____ del 2012

UNIVERSIDAD ESTATAL DE MILAGRO

INSTITUTO DE POSTGRADO Y EDUCACIÓN CONTINUA

Milagro, Abril 2012

CERTIFICACIÓN DE ACEPTACIÓN DEL TUTOR

En calidad de Tutor de Proyecto de Investigación, nombrado por el Comité Técnico del Instituto de Postgrado y Educación Continua, de la Universidad Estatal de Milagro.

CERTIFICO

Que he analizado el Proyecto de Investigación con el tema **ANALISIS DE LA AUDITORIA EN SEGURIDAD INFORMATICA DEL DEPARTAMENTO DE TECNOLOGIAS DE LA UNEMI,** elaborado por el Ing. **JAVIER RICARDO BERMEO PAUCAR,** el mismo que reúne las condiciones y requisitos previos para ser defendido ante el tribunal examinador, para optar por el título de **MAGISTER EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN**

DR. GUSTAVO H. GALIO MOLINA MSc.
C.I: 0906208822

DECLARACIÓN AUTORÍA

La responsabilidad del contenido desarrollado en este Proyecto de Investigación, me corresponden exclusivamente; y la propiedad intelectual del mismo a la Universidad Estatal de Milagro.

ING. JAVIER RICARDO BERMEO PAUCAR
C.I:0919625301

AGRADECIMIENTO

Le agradezco a Dios por tenerme con vida, las bendiciones que me ha dado tener una buena familia que son mis hijos, mi esposa y mis padres, la sabiduría que ha permitido cultivar la honestidad que me ha permitido mantener la fuerza y la tenacidad que hay en mí.

Para todos y cada una de las personas que de una u otra forma colaboraron con los datos para la realización de esta tesis.

A la Universidad Estatal de Milagro y a sus docentes que con sus capacidades, experiencias y orientación nos otorgan sus sabias enseñanzas.

Ing. Javier Ricardo Bermeo Paucar

DEDICATORIA

Dedico este trabajo de tesis a Dios y a mi familia, ya que son los pilares que me motivaron en terminar este gran trabajo, quienes con buen ejemplo de amor, ternura y honradez que me enseñan cada día, que el sacrificio es el camino al éxito y vivir en paz y con tranquilidad. Dedico también a mis compañeros de trabajo de Tecnologías que también aportaron un granito de arena para la culminación de esta tesis brindándome su confianza y buenos deseos**.**

Ing. Javier Ricardo Bermeo Paucar

RESUMEN

La seguridad informática es un tema muy amplio que se enfoca en poder entender que un riesgo y una vulnerabilidad se podrían englobar en una definición más informal que denota la diferencia entre riesgo y vulnerabilidad, de modo que se debe la Vulnerabilidad a una Amenaza y el Riesgo a un Impacto.

La información (datos) se verá afectada por muchos factores, incidiendo básicamente en los aspectos de confidencialidad, integridad y disponibilidad de la misma. Desde el punto de vista de la empresa, uno de los problemas más importantes puede ser el que está relacionado con el delito o crimen informático, por factores externos e internos. Una persona no autorizada podría: Clasificar y desclasificar los datos, Filtrar información, Alterar la información, Borrar la información, Usurpar datos, Hojear información clasificada.

La medida más eficiente para la protección de los datos es determinar una buena política de seguridad informática donde se debe asignar responsabilidades a quienes integren el departamento de sistemas cuyo objetivo principal es salvaguardar la información almacenada en los equipos informáticos mediante técnicas o procedimientos como copias de seguridad o backups (respaldos) Ejm: Copia de seguridad completa, Todos los datos (la primera vez), Copias de seguridad incrementales, Sólo se copian los ficheros creados o modificados desde el último backup (respaldo), Elaboración de un plan de respaldo (backup) en función del volumen de información generada.

ABSTRACT

Computer security is a broad topic that focuses on being able to understand that a risk and vulnerability could cover in a more informal denotes the difference between risk and vulnerability, so must the Vulnerability to a Threat and Risk an impact.

The information (data) will be affected by many factors, focusing primarily on issues of confidentiality, integrity and availability of it. From the point of view of the company, one of the most important may be the one related to the crime or computer crime, for external and internal factors. An unauthorized person may: classify and declassify information, Filtering information, alter information, Clear information, Usurp data Browse classified information.

The most efficient measure to protect data is to determine a good security policy which should assign responsibilities to integrate those systems department whose main purpose is to safeguard the information stored in computer techniques or procedures for backup or backups (backups) Ejm: full backup, all data (first time), incremental backups, only copied the files created or modified since the last backup (backup), Development of a backup plan (backup) depending on the volume of information generated.

ÍNDICE GENERAL

INTRODUCCIÓN **1**
CAPITULO I **3**
EL PROBLEMA **3**
1.1.Situación problemática. 3
1.1.1. Problematización: Origen y descripción del Problema. 3
1.1.2. Delimitación de problema. 9
1.1.3. Determinación del tema. 10
1.2. Pronóstico. 11
1.3. Control de Pronóstico. 12
1.4. Formulación del Problema. 12
1.5. Sistematización del Problema. 12
1.6. Objetivos. 13
1.6.1. Objetivos Generales. 13
1.6.2. Objetivos Específicos. 13
1.7. Justificación. 14
1.7.1. Justificación teórica. 14
CAPITULO II **16**
MARCO TEÓRICO Y CONCEPTUAL **16**
2.1.Marco teórico. 16
2.1.1 Antecedentes históricos. 16
2.1.2 Antecedentes referenciales. 20
2.1.3. Pérdida de información. 22
2.1.4. Antecedentes contextuales. 22
2.2.Marco conceptual. 34
2.3.Hipótesis y Variables. 44
2.3.1. Hipótesis General. 44
2.3.2. Hipótesis Particulares. 44
2.4. Variables. 44
CAPÍTULO III **52**
MARCO METODOLÓGICO **52**
3.1 Tipo, diseño y perspectiva de la investigación. 52

3.2 Población y muestra. 53
3.3 Métodos de investigación. 55
3.3.1 Método teórico. 55
3.3.2 Método Empírico. 56
3.4 Procesamiento de la información. 56
CAPÍTULO IV 57
ANÁLISIS DE LOS RESULTADOS 57
4.1 Análisis de la situación actual. 57
4.2 Comparación, evaluación, tendencia y perspectiva. 58
4.3 Relación entre objeto e hipótesis. 68
4.4 Verificación de las hipótesis. 70
CAPÍTULO V 72
PROPUESTA DE SOLUCIÓN 72
5.1 Titulo de la propuesta. 72
5.2 Fundamentación de la propuesta. 72
5.3 Justificación de la propuesta. 74
5.4 Objetivos de la propuesta. 75
5.4.1. Objetivos Generales. 75
5.4.2. Objetivos Específicos. 75
5.5 Ubicación sectorial y física. 76
5.6 Factibilidad. 76
5.7 Descripción de la propuesta. 78
5.8 Análisis financiero. 82
5.8.1 Inversión Presupuestada del Plan General. 82
5.8.2 Ingresos. 82
5.8.3 Gastos y Costos. 83
5.8.4 Análisis de Factibilidad por Evaluación Financiera. 86
5.8.5 VAN, TIR y Periodo de Recuperación. 88
5.8.6 Flujo de caja. 90
5.9 Ejecución y operación. 91
5.9.1 Ejecución 91
5.10Impacto de la propuesta 185
5.10.1 Análisis del impacto social 185

5.10.2 Análisis del impacto ambiental 185
5.11 Cronograma de la implementación de la propuesta 187
5.12 Lineamiento para evaluar la propuesta.....188
5.13 Conclusión 189
5.14 Recomendaciones 189
Bibliografía 190
Anexo 191

ÍNDICE TABLA

Tabla 1: Justificación de la investigación viabilidad técnica y económica…….. 14
Tabla 2: Diseño de red…….. 36
Tabla 3: Variables Dependientes…… 45
Tabla 4: Variables Independientes…… 46
Tabla 5: Tabla de contingencia general para la comparación de dos variables…….. 47
Tabla 6: Tabla contingencia Confianza en los usuarios con o sin la aplicación de políticas de seguridad informática…… 47
Tabla 7: Tabla contingencia crecimiento económico con Políticas de Seguridad Informática…… 50
Tabla 8: MARCO MUESTRAL: Numero de personal involucrado con los servicios de Tecnología de los Departamentos y Unidades Académicas de la UNEMI…… 51
Tabla 9: Simbología…….. 54
Tabla 10: Conclusiones de Objetivos e Hipótesis…… 68
Tabla 11: Inversión Presupuestada horas extras…… 82
Tabla 12: Gasto Asesoramiento Externo…… 83
Tabla 13: Materiales y Suministros…… 83
Tabla 14: Gasto Pc/servidor…… 83
Tabla 15: Gasto Servicios básicos…….. 84
Tabla 16: Gasto Empleados horas extras…… 85
Tabla 17: Ingresos y Egresos…….. 85
Tabla 18: Utilidad Bruta…… 86
Tabla 19: Periodo de Recuperación…… 88
Tabla 20: Flujo de Caja…… 90
Tabla 21: antenas radiales de la UNEMI……... 102
Tabla 22: Switch de la UNEMI…… 103
Tabla 23: Pach Panel de la UNEMI…… 104
Tabla 24: Servidor web…… 106
Tabla 25: Servidor Base de Datos…….. 107

Tabla 26: Servidor Preproducción y Desarrollo…… 107
Tabla 27: Servidor Base de Datos Web…… 107
Tabla 28: Servidor Mail, PDC Y LDAP…… 108
Tabla 29: Servidor Proxy…….. 108
Tabla 30: Servidor DHCP y Router…… 109
Tabla 31: Servidor Firewall…….. 109
Tabla 32: Servidor Clientes Livianos…….. 110

ÍNDICE GRÁFICO

Gráfico 1: Amenazas para la seguridad……..... 6
Gráfico 2: Capas lógicas……... 35
Gráfico 3: Gráfico conectividad entre edificios…… 37
Gráfico 4: Conocimiento de que es una auditoria de sistemas…… 58
Gráfico 5: Sistemas informáticos que utilizan para su trabajo…… 59
Gráfico 6: Nivel de importancia de los servicios informáticos del TIC's…… 60
Gráfico 7: Satisfacción Usuarios en capacitaciones y Soporte Técnico…… 61
Gráfico 8: Conocimiento de la existencia del Dpto. Auditoría Interna…… 62
Gráfico 9: Conoce de sistema seguridad en el Dpto. TIC's…… 63
Gráfico 10: Importancia sistemas Informáticos como herramienta de trabajo…. 64
Gráfico 11: Información confiable de los sistemas informáticos…… 65
Gráfico 12: Importancia a la auditoría al departamento del TIC's…… 66
Gráfico 13: Ubicación de la Universidad Estatal de Milagro (Ubicación geográfica)…… 76
Gráfico 14: Normativa Legislación del Ecuador…… 80
Gráfico 15: Infracciones Informáticas…… 80
Gráfico 16: Comparativo de Ingresos y Egresos…… 86
Gráfico 17: Organigrama del Departamento del TIC's…… 95

INTRODUCCIÓN

Actualmente la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y nuevas plataformas informáticas disponibles, buscando proteger los datos, de la aparición de nuevas amenazas en los sistemas informáticos. Esto ha llevado a que muchas organizaciones hayan desarrollado documentos y directrices que orientan en el uso adecuado de estas tecnologías para obtener el mayor provecho de las ventajas que brindan. De esta manera, las políticas de seguridad informática surgen como una herramienta para concienciar, al departamento de Tecnología de la Universidad Estatal de Milagro, sobre la importancia en aplicar controles de seguridad para proteger información sensible y/o servicios críticos, que permiten a la universidad desarrollarse eficientemente en el sector de la educación.

Las políticas de seguridad informática fijan los mecanismos y procedimientos que debe adoptar el departamento de Tecnologías de la UNEMI para salvaguardar sus sistemas y la información que estos contienen. Éstas políticas deben diseñarse "a medida" para así recoger las características propias de cada departamento. No son una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, son más bien una descripción de lo que se debe proteger y el por qué de ello, por lo que pueden tomarse como una forma de comunicación entre los operadores y los directores. De acuerdo con lo anterior, el aplicar una auditoria de seguridad informática requiere un alto compromiso de los principales directivos de la UNEMI, explotar las destrezas, habilidades y experiencia técnica de los usuarios; detectar fallas, debilidades, y revisiones periódicas que permitan actualizar dichas políticas en función del dinámico ambiente que rodea las organizaciones modernas.

Para la revisión de las políticas aplicadas en el área informática, resulta conveniente la ejecución de una auditoría de seguridad informática en la Universidad Estatal de Milagro. Es una disciplina que, a través de personas independientes de la operación

auditada y mediante el empleo de técnicas y procedimientos adecuados, evalúa el cumplimiento de los objetivos de la institución con respecto a la seguridad de la información y emitir recomendaciones que contribuyen a mejorar su nivel de cumplimiento.

CAPITULO I

EL PROBLEMA

1.1. Situación problemática.

1.1.1. Problematización: Origen y descripción del Problema.

Para comenzar el análisis de la Seguridad Informática se deberá conocer las características de lo que se pretende proteger, los servidores de datos y equipos de computación en el Departamento de Tecnologías y Comunicaciones de la UNEMI.

En la actualidad el departamento de Tecnología de Información y Comunicaciones de la UNEMI no cuenta con políticas de seguridad informática, ya que el acceso a todas sus áreas físicas, lo puede realizar cualquier personal de la UNEMI y en muchas de las ocasiones, personas particulares; ya que no cuenta con una herramienta que pueda controlar su ingreso o políticas de seguridad normadas que prohíba el acceso al departamento y a servidores de datos o información.

El personal que trabaja en el Departamento de Tecnologías está consciente del riesgo que conlleva no tener políticas de seguridad, y han venido trabajando con una seguridad relativamente aprendida en sus estudios universitarios y del conocimiento aprendido de otras empresas por lo que es recomendable la aplicación de una auditoria informática en el departamento.

Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se la valora adecuadamente debido a su intangibilidad, lo que no ocurre con los equipos, las aplicaciones y la documentación.

Existe Información que debe o puede ser pública, ser visualizada por cualquier persona (por ejemplo listados de estudiantes matriculados, notas, etc.). Aquella que debe ser privada, sólo debe ser visualizada por el grupo selecto de personas que trabaja con ella (por ejemplo, actas de grado ingresados por los profesores, roles de pagos, facturas, etc.). En esta última debemos maximizar nuestros esfuerzos para

reservarla de ese modo, reconociendo las siguientes características en la Información:

1. Crítica: es indispensable para garantizar la continuidad operativa.
2. Valiosa: es un activo con valor en sí misma de la Institución.
3. Sensitiva: debe ser conocida por las personas que la procesan y sólo por ellas.

La integridad de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla en la integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

La disponibilidad y operatividad de la Información, es la capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y software funcionando correctamente, y que se respeten los formatos para su recuperación en forma satisfactoria.

La privacidad o confidencialidad de la Información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la Información puede provocar severos daños a su dueño (por ejemplo conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se “filtran” a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes).

El control sobre la información permite asegurar que sólo los usuarios administradores pueden decidir cuándo y cómo permitir el acceso a la misma.

La autenticidad permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución.

Adicionalmente pueden considerarse algunos aspectos adicionales, relacionados con los anteriores, pero que incorporan algunos aspectos particulares:

• **Protección a la Réplica:** mediante la cual se asegura que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.

• **No Repudio:** Mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.

• **Consistencia:** se debe poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.

• **Aislamiento:** este aspecto, íntimamente relacionado con la confidencialidad, permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.

• **Auditoria:** es la capacidad de determinar qué acciones o procesos se están llevando a cabo en el sistema, así como quién, como y cuando las realiza.

Cabe definir amenaza, en el entorno informático, como cualquier elemento que comprometa en su integridad al sistema.

Las amenazas pueden ser analizadas en tres momentos: antes del ataque, durante y después del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

a. **La Prevención (antes):** mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión.

b. **La Detección (durante):** mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.

c. **La Recuperación (después):** mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal. Por ejemplo recuperación desde las copias de seguridad (backup) realizadas.

Gráfico 1: Amenazas para la seguridad.

Las preguntas que se hace un técnico en sistemas de información ante un problema de seguridad informática, normalmente, están relacionadas con medidas defensivas que no solucionan un problema dado, sólo lo transforma o retrasa. La amenaza o riesgo sigue allí y las preguntas que este técnico debería hacerse son:

• ¿Cuánto tardará la amenaza en superar la “solución” planteada?
• ¿Cómo se hace para detectarla e identificarla a tiempo?
• ¿Cómo se hace para neutralizarla o bloquearla?

Para responderlas definiremos riesgo como “la proximidad o posibilidad de daño sobre un bien”.

Ya se trate de actos naturales, errores u omisiones humanas y actos intencionales, cada riesgo debería ser enfrentado de las siguientes maneras:

1. Minimizando la posibilidad de su ocurrencia.
2. Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
3. Diseño de métodos para la más rápida recuperación de los daños experimentados.

4. Corrección de las medidas de seguridad en función de la experiencia recogida.

Luego, el daño es el resultado de la amenaza; aunque esto es sólo la mitad del axioma.

El daño también es el resultado de la no–acción, o acción defectuosa, del protector. El daño puede producirse porque el protector no supo identificar adecuadamente la amenaza y, si lo hizo, se impusieron criterios por encima de la seguridad. De allí que se deriven responsabilidades para la amenaza (por supuesto) pero también para la figura del protector.

Luego, el protector será el encargado de detectar cada una de las Vulnerabilidades (debilidades) del sistema que pueden ser explotadas y empleadas, por la amenaza, para comprometerlo. También será el encargado de aplicar las Contramedidas (técnicas de protección) adecuadas.

El nivel seguridad indicara el índice en que un Sistema Informático está libre de todo peligro, daño o riesgo. Esta característica es muy difícil de conseguir (según los especialistas imposible [xx]) en un 100% por lo que sólo se habla de Fiabilidad y se la define como “la probabilidad de que un sistema se comporte tal y como se espera de é, y se habla de Sistema Fiable en vez de sistema seguro.

Luego para garantizar que un sistema sea fiable se deberá garantizar las características de Integridad, Operatividad, Privacidad, Control, No repudio y Autenticidad. Se deberá conocer “qué es lo que queremos proteger” en este caso es la Información y equipos de computación, “de quién lo queremos proteger”, personal interno y externo de la UNEMI, “cómo se puede lograr esto técnicamente” aplicando normativas y políticas de seguridad informáticas; para luego concluir con la formulación de estrategias adecuadas de seguridad tendientes a la disminución de los riesgos que presenta actualmente en la Institución.

Comprender y conocer sobre seguridad ayudará a llevar a cabo análisis de los Riesgos, las Vulnerabilidades, Amenazas y Contramedidas; evaluar las ventajas o

desventajas de la situación; decidir medidas, informáticas, técnicas, físicas, tácticas metodológicas, en base de las necesidades de seguridad.

Es importante remarcar que cada unas de estas técnicas parten de la premisa de que no existe el 100% de seguridad esperado o deseable, en estas circunstancias que todo va evolucionando o cambiando, nos conlleva a que cada día se debe ir actualizando las normativas y políticas de seguridad informática.

Se entiende como seguridad un estado de cualquier tipo de información (informático o no) que nos indique, que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo a los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en informática es irreal porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

- **Integridad**: La información sólo puede ser modificada por quien está autorizado y de manera controlada.
- **Confidencialidad**: La información sólo debe ser visible para los autorizados.
- **Disponibilidad**: Debe estar disponible cuando se necesita.
- **Irrefutabilidad** (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Dependiendo de las fuentes de amenaza, la seguridad puede dividirse en tres partes: seguridad física, seguridad ambiental y seguridad lógica.

En estos momentos la seguridad informática es un tema de dominio obligado por cualquier usuario de Internet, para no permitir que su información sea comprometida.

Términos relacionados con la seguridad informática

- **Activo**: recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

- **Amenaza**: es un evento que puede desencadenar un incidente en la organización, puede producir daños materiales o pérdidas inmateriales en sus activos.
- **Impacto**: medir la consecuencia al materializarse una amenaza.
- **Riesgo**: Es la probabilidad de que suceda la amenaza o evento no deseado
- **Vulnerabilidad**: Son aspectos que influyen negativamente en un activo y que posibilita la materialización de una amenaza.
- **Ataque**: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
- **Contingencia**: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Fuente: Investigación por observación directa en el departamento del TIC's de la UNEMI.

1.1.2. Delimitación de problema.

CAMPO: Universidad Estatal de Milagro.
ÁREA: Departamento de Tecnología de la Información y Comunicaciones.
ASPECTO: Mejorar la Seguridad Informática dentro y fuera del Departamentos TIC's y así conseguir los objetivos planteados.
TEMA: Análisis de la Auditoria de Seguridad Informática del Departamento de Tecnologías en la Universidad Estatal de Milagro.

Durante los últimos años de nuestra carrera nos planteamos el interrogante sobre la Temática a desarrollar en el trabajo final, y nos propusimos varios objetivos que queríamos cumplir.

Se tiene la intención de aprender nuevos conceptos que no se haya desarrollado durante el transcurso de la carrera, y se quiere realizar un trabajo de investigación para ejercitar el auto aprendizaje adquirido en el ambiente universitario.

El tema a desarrollar debía ser de actualidad, innovador; y poder aplicarse a la realidad, poder ser llevado a la práctica con conocimientos adquiridos y afrontar así

el desenvolvimiento en esta materia. Por último, permita ayudar a construir el perfil técnico como futuros profesionales.

Todas estas razones se encaminan hacia la Seguridad Informática, lo que permite plasmar la investigación en un enfoque enteramente práctico.
Como actividad inicial se desarrolla una auditoría de seguridad, con el fin de evaluar la consistencia de los sistemas de información y de control; la eficiencia, efectividad de los programas, y el cumplimiento de los reglamentos y normas de seguridad. Todo esto con el fin de definir las políticas que conformen un plan de seguridad informático.

El paso siguiente es, establecer estándares de protección de los recursos informáticos en la universidad, y sería la creación de los manuales de procedimientos y políticas, tarea que se verá facilitada para la auditoría de seguridad que se realizada en el presente trabajo.

ASPECTO:
Análisis de la Auditoria de Seguridad Informática del Departamento de Tecnologías en la Universidad Estatal de Milagro, a través de técnicas y procedimientos establecidos con normas internacionales de seguridad de información.

TEMA:
Análisis de la Auditoria de Seguridad Informática del Departamento de Tecnologías en la Universidad Estatal de Milagro.

1.1.3. Determinación del tema.

Una Auditoria de seguridad informática es una forma de ver, que está fallando o que recursos no se está aplicando de una mejor manera, ya que si no se tiene una política de seguridad informática, no se sabe que está recurriendo mal, ya que las mismas establecen un canal formal de seguridad, en relación con los recursos y servicios informáticos de la institución.

El no contar con normas y políticas de seguridad, se incurre a cometer inconscientemente errores sin responsabilidad alguna.

1.2. Pronóstico.

La auditoria en seguridad informática, debe orientar las decisiones que se toman en relación, con las políticas y procedimientos de seguridad informática, se requiere la disposición de todos los miembros de la Institución para lograr una visión conjunta de lo que se considera importante.

La auditoria de Seguridad Informática debe considerar principalmente los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Por último, y no menos importante, es que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, etc.

1.3. Control de Pronóstico.

Auditar y analizar la seguridad informática que tiene el Dpto. de Tecnología de la Información y Comunicaciones comparada con otras Universidades o Instituciones públicas que tengan una buena aplicación de políticas y procedimientos con respecto a la seguridad informática.

Con los resultados obtenidos establecer políticas y procedimientos de seguridad informática, demostrando las ventajas que significa contar con este tipo de normas, políticas y procedimientos en la Universidad.

1.4. Formulación del Problema.

¿Qué factores están influyendo para que el Departamento de TIC's de la UNEMI, no hayan tomado la decisión de realizar una auditoría de seguridad informática para salvaguardar la información y el ingreso a lugares restringidos.

1.5. Sistematización del Problema.

1. ¿De qué forma influye en el Departamento del TIC'S, el no contar con políticas y procedimientos de seguridad informática?

2. ¿Cómo afecta, el no tener políticas y procedimientos de seguridad informática en el Departamento del TIC'S de la UNEMI?

3. ¿Qué efecto está incidiendo en los diferentes departamentos de la UNEMI el no contar con una política de seguridad de información?

4. ¿De qué forma se establecería una estrategia para realizar una auditoría de seguridad informática en el Departamento del TIC'S de la UNEMI y mejorar el desempeño laboral?

1.6. Objetivos.

1.6.1. Objetivos Generales.

El objetivo general consiste en la realización de una Auditoría Informática en el Departamento de Tecnología de la Información y Comunicaciones de la UNEMI con el fin de revelar las vulnerabilidades existentes en lo relativo a controles de seguridad, como medio para el desarrollo de una Política de Seguridad, donde se definirán los lineamientos para promover la implementación de un modelo de seguridad en toda la Universidad.

1.6.2. Objetivos Específicos.

- Analizar cómo influye el no contar con una auditoria de seguridad informática sobre Políticas y Procedimientos que debe aplicarse en el Departamento del TIC'S de la UNEMI.
- Delimitar como está afectando negativamente no contar con una auditoria de seguridad informática en el Departamento del TIC'S de la UNEMI.
- Establecer una propuesta Tecnológica de una auditoria de seguridad informática para mejorar el desempeño laboral de los departamentos de la Universidad Estatal de Milagro si tuvieran un manual de Seguridad Informática.
- Establecer una estrategia para proponer a el Departamento del TIC'S de la UNEMI; una auditoria de seguridad informática.

1.7. Justificación.

1.7.1. Justificación teórica.

1.7.1.1 Justificación de la investigación viabilidad técnica y económica.

Desde 1950	Desde 1980	Desde1990	Desde1995
1ª GENERACIÓN	**2ª GENERACIÓN**	**3ª GENERACIÓN**	**4ª GENERACIÓN**
Aplicaciones	Bases de datos	Redes y	Telecomunicaciones
Aisladas	e integración	Terminales	Digitalización
			Internet
			Rediseño procesos
		Procesos Comerciales	
	Procesos de gestión		
	Procesos administrativos		

Tabla 1: Justificación de la investigación viabilidad técnica y económica.

Hoy en día, los progresos informáticos denominadas tecnologías de la información, que abarcan los equipos y aplicaciones informáticas, están teniendo un gran efecto. De hecho, se dice que estamos en un nuevo tipo de sociedad llamada Sociedad de la información o Sociedad del Conocimiento.

Teniendo en cuenta lo mencionado, no se puede dejar de considerar la seguridad de la información, se pretende que la información que hasta hoy era considerada privada, no caiga en manos equivocadas, o que se encontrase sorpresivamente el sistema de información inutilizado por la acción de algún código malicioso que pretende tomar el control de la máquina o simplemente sacarla de circulación, por ejemplo, generando procesos basura.

Se detallan las pautas necesarias para conseguir un nivel de seguridad aceptable protegiendo los sistemas informáticos de las debilidades más comunes que día a día se hacen públicas a través del mismo sistema de red. Con este trabajo no se

pretende construir un instructivo camuflado de cómo hackear una máquina para personas poco capaces, sino comprender que se puede incrementar el nivel de seguridad de una computadora, trabajando de forma ordenada y con varios cambios, para así lograr sistemas fiables y robustos.

Al establecer políticas de seguridad informática, se debe ofrecer explicaciones comprensibles sobre por qué deben tomarse decisiones y explicar la importancia de los recursos. Igualmente, deberán establecerse las expectativas sobre seguridad de la Universidad en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, etc.

CAPITULO II

MARCO REFERENCIAL

2.1. Marco teórico.

2.1.1 Antecedentes históricos.

2.1.1.1 Influencia de la tecnología en el Entorno.

El progreso tecnológico, con la informática, la robótica, el diseño y la fabricación asistida por ordenador, la telemática, etc., supone una profunda transformación del sistema productivo de las empresas, y provoca que la innovación tecnológica escape al dominio de la mayor parte de las empresas y se transforme en un imperativo para el crecimiento y la supervivencia, por tal motivo, se realizara una investigación del problema previamente.

Aproximadamente trescientos millones de personas están conectadas a Internet, la tecnología informática no ha parado de avanzar durante cuarenta años de progresos agigantados. La combinación de nuevos avances en muchas áreas de la tecnología convergiendo en el inicio del nuevo milenio, continuará revolucionando el mundo de los negocios, en una escalada sin precedentes.

Los campos más importantes que se centrarán en el futuro en los desarrollos tecnológicos son: la energía nuclear, las fuentes alternativas de energía no renovables, la robótica, la biotecnología, la informática, el láser y sus aplicaciones a los campos de las comunicaciones, la medicina e industria**,** las comunicaciones, la genética (ADN, Acido Desoxirribonucleico), la química, la física, el comportamiento de sistemas disipativos, la física cuántica y las partículas subatómicas, la clonación, los estudios de comportamiento del cerebro, la inteligencia artificial, la nanotecnología, los superconductores, los nuevos materiales, etc.

2.1.1.1.1 Beneficios de la tecnología en la seguridad informática.

Las Universidades cuentan con importantes ventajas: agilidad de adaptación al cambio, capacidad de crecimiento y programas de apoyo. Pero tienen un gran inconveniente: la resistencia y aversión a la tecnología.

La incorporación de nuevas herramientas se produce más por imitación que por planteamientos estratégicos. Hay que aprender a beneficiarse de su utilidad. Las Universidades carecen de seguridad informática capaz de controlar y regularizar la fuga de información y respaldo del mismo. Todas manifiestan un gran interés por la información y las tecnologías relacionadas, sin embargo, desconocen de normas, políticas y procedimientos que pueden utilizar por el beneficio de salvaguardar información que tiene que ver directamente con la administración y toma de decisiones departamentales.

Estos riesgos que se enfrentan ha llevado a que se desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de las ventajas, y evitar el uso indebido de la misma, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la Universidad.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia de la información, y servicios críticos que permitan a la UNEMI, crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para detectar fallas y debilidades en la seguridad, y constancia para renovar y actualizar las normas y políticas de seguridad.

Proteger de virus, tener una mejor comunicación y control, son algunas de las posibilidades que buscan las tecnologías de información. En algunos casos las T.I. sólo se ven como una posible ventaja competitiva a futuro.

2.1.1.1.2 Tecnologías de Información políticas se seguridad Informática.

Los beneficios de un sistema de seguridad informática bien elaborados son inmediatos, ya que la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- Aumento de la productividad.
- Aumento de la motivación del personal.
- Compromiso con la misión de la compañía.
- Mejora de las relaciones laborales.
- Ayuda a formar equipos competentes.
- Mejora de los climas laborales para los RR.HH.

2.1.1.1.3 Opciones para establecer Seguridad Informática

Para que el plan de seguridad informática entre en vigor y los elementos empiecen a funcionar, se observen y acepten en las nuevas instituciones, leyes y costumbres del nuevo sistema de seguridad se deben seguir los siguientes 8 pasos:

1. Introducir el tema de seguridad en la visión de la empresa.
2. Definir los procesos de flujo de información y sus riesgos en cuanto a todos los recursos participantes.
3. Capacitar a los gerentes y directivos, bajo un enfoque global
4. Designar y capacitar supervisores de área.
5. Definir y trabajar sobre todo las áreas donde se pueden lograr mejoras relativamente rápidas.
6. Mejorar las comunicaciones internas.
7. Identificar claramente las áreas de mayor riesgo corporativo y trabajar con ellas planteando soluciones de alto nivel.
8. Capacitar a todos los trabajadores en los elementos básicos de seguridad y riesgo para el manejo del software, hardware y con respecto a la seguridad física.

Desde el punto de vista de una auditoria de seguridad informática, se debe contar con un conjunto de disposiciones o cursos de acción para llevarse a cabo en caso de presentarse situaciones de riesgo, a saber:

- Obtener una especificación de las aplicaciones, los programas y archivos de datos.
- Aplicar medidas en caso de desastre como pérdida total de datos, abuso y los planes necesarios para cada caso.
- Definir prioridades en cuanto a acciones de seguridad de corto y largo plazo.
- Verificar el tipo de acceso que tiene las diferentes personas de la organización, cuidar que los programadores no cuenten con acceso a la sección de operación y viceversa.
- Definir que los operadores no sean los únicos en resolver los problemas que se presentan.

2.1.1.2 La revolución Tecnológica.

En el mundo industrial avanzado, las máquinas realizan la mayor parte del trabajo agrícola e industrial. Con la ayuda de máquinas controladas por ordenadores, las empresas pueden producir bienes únicos a menor costo, adecuando rápidamente la oferta a la demanda del mercado.

El mayor peso relativo está puesto en la innovación, por lo cual se aplica a un proceso de desindustrialización; las compañías disminuyen su tamaño, para facilitar la circulación de la información, hacia los centros de decisión que poseen el conocimiento, para asignarle valor; se tercealiza su servicio (outsourcing), o las actividades de producción, mantenimiento, o distribución y se invierten recursos en investigación y desarrollo, buscando generar un aumento o mejorar la “recordación de marca”, mientras se eleva el estatus del cliente utilizando tecnología como soporte (personalización masiva).

Los trabajadores producen más bienes que hace un siglo, invirtiendo menos horas de trabajo, las personas han ampliado su expectativa de vida y viven este tiempo de forma más sana, como resultado de la tecnología. La invención del automóvil, la

radio, la televisión y teléfono revolucionó el modo de vida y de trabajo de millones de personas.

En el siglo XX los logros tecnológicos fueron insuperables, con un ritmo de desarrollo mucho mayor que en períodos anteriores. La economía es un vasto sistema interconectado en el que todo recurso que se libera queda a disposición de otra área económica que le encuentra valor.

De esto, se desprende la idea, de que cuando se producen cambios por aplicación de tecnología, simultáneamente se están creando nuevos puestos de trabajo.

A partir de la década del 70, se han observado cambios en el mercado laboral:

- Diversidad de la fuerza de trabajo, lo que significa una mayor heterogeneidad en términos de sexo, edad, raza, etnia; producto, en gran medida, de las migraciones desde las regiones periféricas, hacia los países más desarrollados. Concretamente, se observa: Un acceso creciente de las mujeres a trabajos no hogareños (sobre todo en los países más desarrollados) y nuevas generaciones en busca de empleos (sobre todo en los países menos desarrollados).
- Nuevos y rápidos aportes de adelantos tecnológicos: mecanización, robotización y automatización que reemplazan a la mano de obra convencional, especialmente la menos cualificada y remunerada.
- En el caso de las pequeñas empresas o de los países con menor capacidad de desarrollo tecnológico, han optado por competir reestructurándose, reduciendo la incidencia de la mano de obra en su producción, haciendo “más o igual, con menos gente” e inclusive pagándoles menos que antes del ajuste.

2.1.2 Antecedentes referenciales.

2.1.2.1 Proceso Administrativo.

Las diversas funciones del administrador, en conjunto, conforman el proceso administrativo. Por ejemplo, planeación, organización, dirección y control,

consideradas por separado, constituyen las funciones administrativas, cuando se toman como una totalidad para conseguir objetivos, conforman el proceso administrativo.

2.1.2.1.1 Planeación.

“La planeación consiste en fijar el curso concreto de acción que ha de seguirse, estableciendo los principios que habrán de orientarlo, la secuencia de operaciones para realizarlo, y la determinación de tiempos y números necesarios para su realización “.A. Reyes Ponce [1].

“La planeación es el primer paso del proceso administrativo por medio del cual se define un problema, se analizan las experiencias pasadas y se esbozan planes y programas” J. A. Fernández Arenas [2].

2.1.2.1.2 Organización.

“Organizar es agrupar y ordenar las actividades necesarias para alcanzar los fines establecidos creando unidades administrativas, asignando en su caso funciones, autoridad, responsabilidad y jerarquía, estableciendo las relaciones que entre dichas unidades debe existir.” Eugenio Sixto Velasco [3].

“Organización es la coordinación de las actividades de todos los individuos que integran una empresa con el propósito de obtener el máximo de aprovechamiento posible de elementos materiales, técnicos y humanos, en la realización de los fines que la propia empresa persigue” Issac Guzmán V [4].

2.1.2.1.3 Dirección.

“Consiste en coordinar el esfuerzo común de los subordinados, para alcanzar las metas de la organización”. Burt K. Scanlan[5].

“Consiste en dirigir las operaciones mediante la cooperación del esfuerzo de los subordinados, para obtener altos niveles de productividad mediante la motivación y supervisión”. Lerner y Baker [6].

2.1.3 Perdida de información.

“Cuando se trata de prevenir la pérdida de información, el aspecto más importante es la falta de control en la comunicación”, comentó Tom Gillis [7], Vicepresidente Sénior de Mercadotecnia de IronPortSystems. “Los comunicados electrónicos y el intercambio de la información constituyen el sector de pérdida de información más importante para las empresas. Actualmente, los firewalls y otras soluciones de seguridad para redes no incluyen capacidades para prevenir la pérdida de información y asegurar el intercambio de datos. Se necesitan controles eficaces como el escaneo de contenido para proteger mensajes que contengan información confidencial y codificada.

Cuando se está buscando una solución para controlar la pérdida de información, es necesario que las organizaciones consideren las mejores prácticas para estructurar una solución que se adapte a sus necesidades específicas”.

2.1.4 Antecedentes contextuales.

2.1.4.1 Riesgos Informáticos.

El reporte titulado “Data Loss Prevention Best Practices, Managing Sensitive Data in the Enterprise”, de Bradley R. Hunter [8] define algunas de las mejores prácticas que pueden aplicar las empresas para prevenir las pérdidas de información, asegurar el cumplimiento y proteger el valor y la reputación de su marca, dicho reporte es elaborado por Iron Port Systems.

La Prevención de la Pérdida de Información (DLP, Data Loss Prevention, por sus siglas en inglés) es un serio problema para las instituciones; la cantidad de incidentes y costos relacionados continúan aumentando. Puede tratarse de un ataque malintencionado o un error involuntario, pero la pérdida de información puede

afectar la marca, disminuir el valor de todas las partes involucradas y dañar el buen nombre y la reputación de una institución.

La gran mayoría de medios de transmisión electrónica, como los correos electrónicos, mensajes instantáneos, webmails, formatos en sitios web o transferencias de archivos que utiliza una empresa no están sujetos a un control o monitoreo, por lo tanto, siempre existe el riesgo de que la información confidencial caiga en las manos equivocadas. En todos los protocolos básicos de cualquier empresa siempre se debe incluir una solución inteligente y de alto rendimiento.

Los líderes deben buscar proveedores con gran experiencia y conocimientos en el escaneo de contenido para seleccionar la mejor solución disponible.

2.1.3.2 Evolución de la Comunicación en el desarrollo tecnológico.

La evolución de la comunicación humana desde la perspectiva tecnológica está en una búsqueda constante del hombre por satisfacer cada vez mejor su necesidad de comunicación ha sido el impulso que ha logrado la instauración en el mundo de instrumentos cada día más poderosos y veloces en el proceso comunicativo.

Sólo basta una retrospectiva para definir cómo el ser humano ha logrado evolucionar sus formas de comunicación: Desde rudimentarios métodos como la escritura jeroglífica, pasando por la invención del alfabeto y del papel, dando un leve salto hasta la llegada de la imprenta, y apenas uno más para la aparición del teléfono, el cine, la radio y la televisión.

Todos estos instrumentos han sido ciertamente un avance en las formas de comunicación del hombre y, prácticamente todos, han sido posibles gracias a la tecnología, que a su vez ha sido el instrumento cuya evolución ha determinado el avance de la humanidad.

Una red de área local, red local o LAN (del inglés Local Área Network) es la interconexión de varios ordenadores y periféricos. Su extensión está limitada

físicamente a un edificio o a un entorno de 200 metros o con repetidores podríamos llegar a la distancia de un campo de 1 kilómetro.

Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

Evolución.

Las primeras redes fueron de tiempo compartido las mismas que utilizaban mainframes y terminales conectadas.

Su entorno se implementaba con la SNA (System Network Architecture o Arquitectura de Sistemas de Redes) de IBM y la arquitectura de red Digital.

Las LANs (Local Area Networks o Redes de Área Local) surgieron a partir de la revolución de la PC. Las LANs permitieron que usuarios ubicados en un área geográfica relativamente pequeña pudieran intercambiar mensajes y archivos, y tener acceso a recursos compartidos de toda la Red, tales como Servidores de Archivos o de aplicaciones.

Con la aparición de NetWare surgió una nueva solución, la cual ofrecía: soporte imparcial para los más de cuarenta tipos existentes de tarjetas, cables y sistemas operativos mucho más sofisticados que los que ofrecían la mayoría de los competidores. NetWare dominaba el campo de las LAN de los ordenadores personales desde antes de su introducción en 1983 hasta mediados de los años 1990, cuando Microsoft introdujo Windows NTAdvance Server y Windowsfor Workgroups.

De todos los competidores de NetWare, sólo BanyanVINES tenía poder técnico comparable, pero Banyan ganó una base segura. Microsoft y 3Com trabajaron juntos

para crear un sistema operativo de red simple el cual estaba formado por la base de 3Com's 3+Share, el Gestor de redes LAN de Microsoft y el Servidor del IBM. Ninguno de estos proyectos fue muy satisfactorio.

Ventajas.

En una empresa suelen existir muchos ordenadores, los cuales necesitan de su propia impresora para imprimir informes (redundancia de hardware), los datos almacenados en uno de los equipos es muy probable que sean necesarios en otro de los equipos de la empresa, por lo que será necesario copiarlos en este, pudiéndose producir desfases entre los datos de dos usuarios, la ocupación de los recursos de almacenamiento en disco se multiplican (redundancia de datos), los ordenadores que trabajen con los mismos datos tendrán que tener los mismos programas para manejar dichos datos (redundancia de software), etc.

La solución a estos problemas se llama red de área local, esta permite compartir bases de datos (se elimina la redundancia de datos), programas (se elimina la redundancia de software) y periféricos como puede ser un módem, una tarjeta RDSI, una impresora, etc. (se elimina la redundancia de hardware); poniendo a nuestra disposición otros medios de comunicación como pueden ser el correo electrónico y el Chat. Nos permite realizar un proceso distribuido, es decir, las tareas se pueden repartir en distintos nodos y nos permite la integración de los procesos y datos de cada uno de los usuarios en un sistema de trabajo corporativo. Tener la posibilidad de centralizar información o procedimientos facilita la administración y la gestión de los equipos.

Además una red de área local conlleva un importante ahorro, tanto de tiempo, ya que se logra gestión de la información y del trabajo, como de dinero, ya que no es preciso comprar muchos periféricos, se consume menos papel, y en una conexión a Internet se puede utilizar una única conexión telefónica o de banda ancha compartida por varios ordenadores conectados en red.

Características importantes.

- Tecnología broadcast (difusión) con el medio de transmisión compartido.

- Capacidad de transmisión comprendida entre 1 Mbps y 1 Gbps.
- Extensión máxima no superior a 3 km (una FDDI puede llegar a 200 km)
- Uso de un medio de comunicación privado
- La simplicidad del medio de transmisión que utiliza (cable coaxial, cables telefónicos y fibra óptica)
- La facilidad con que se pueden efectuar cambios en el hardware y el software
- Gran variedad y número de dispositivos conectados
- Posibilidad de conexión con otras redes
- Limitante de 100 m

2.1.3.3 Los medios de comunicación y su relación con las tecnologías de información.

En este sentido, Cordeiro [9] (1998) señala que "La historia de la humanidad ha sido un proceso largo y complejo a través de muchos miles de años. Dicho proceso no ha sido lineal sino que, por el contrario, ha pasado por grandes revoluciones que han transformado completamente la forma en que los seres humanos se relacionan con el universo, cuya historia es muchísimo más larga."

Cordeiro divide la historia de la evolución humana en tres etapas que califica como revoluciones, cada una de ellas caracterizada por una invención o nueva tecnología, a su vez relacionadas con alguna nueva forma de comunicación.

2.1.3.3.1 Revolución Agrícola.

La primera fue la Revolución Agrícola, a partir del año 8000 A.C. cuando el hombre inventa la agricultura e inicia una nueva forma de vida: deja de ser nómada, abandona su etapa primitiva, comienza a formar comunidades estables y aparecen las primeras ciudades. El hombre hace de la agricultura su principal forma de sustento y, con ella, aparece también la ganadería y un poco después el comercio.

La necesidad de contar, obliga a la invención de los números, los cuales evolucionan hasta dar origen a la escritura (cuneiforme y jeroglífica). Hacia el año 1000 A.C. los fenicios inventan el alfabeto, un conjunto de grafías que permite la representación de sonidos.

Así, se conoce a la escritura como el hecho más trascendental de la revolución agrícola y, además de ser inclusive el punto de inicio de la historia misma de la humanidad, representa el primer gran avance tecnológico logrado por el hombre en su proceso de comunicación.

2.1.3.3.2 Revolución de la humanidad.

La segunda revolución de la humanidad, según la cronología de Cordeiro [10], es la Revolución Industrial, que precisamente marca su inicio a partir de la invención de la imprenta de Johannes Gutenberg en los años 1400 D.C. Con la imprenta se inicia una nueva etapa caracterizada por la masificación del conocimiento, porque crece el número de personas con acceso a la información escrita. Además comienzan a plasmarse los nuevos conocimientos teóricos y surgen nuevos desarrollos tecnológicos: La máquina sumadora, el reloj mecánico, la máquina de coser. Se dieron en esta etapa también importantes descubrimientos en biología, electricidad, química, medicina; todos con posibilidades de perdurar y darse a conocer gracias a la imprenta: El segundo gran paso tecnológico del hombre en la evolución de su proceso comunicativo.

2.1.3.3.3 Revolución de la Inteligencia.

La tercera revolución, en la cual se encuentra inmersa aún la humanidad, es la Revolución de la Inteligencia. Cordeiro explica que esta última revolución se centra en el ser humano, en su capacidad de comunicarse y transformarse, y que la riqueza ya no estará determinada por el dinero y por las posesiones materiales sino por el conocimiento. La revolución de la inteligencia de Cordeiro es análoga a la denominada Tercera Ola de AlvinToffler o a la Aldea Global de Mc Luhan [11].

2.1.3.4 Tecnología de información.

En tal sentido, Canga Larequi [12], (1988) define la tecnología de información y comunicación, como un estudio sistematizado del conjunto de procedimientos que están al servicio de la información y la comunicación. Pero la concepción de Tecnologías de Información y Comunicación no puede verse de manera aislada porque se trata de una definición que se enmarca dentro de las actividades humanas. Es así como los avances en la tecnología, aplicada al proceso

comunicativo dependen en cierta medida de los avances tecnológicos que la humanidad logre en otras áreas del conocimiento científico, y, esta evolución, es la que ha permitido que el proceso comunicativo del hombre tenga hoy características casi ilimitadas en cuanto a tiempo y espacio.

2.1.3.5 Qué es la interconexión de redes.

Cuando se diseña una red de datos se desea sacar el máximo rendimiento de sus capacidades. Para conseguir esto, la red debe estar preparada para efectuar conexiones a través de otras redes, sin importar qué características posean.

El objetivo de la Interconexión de Redes (Internetworking) es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías de forma transparente para el usuario. Este concepto hace que las cuestiones técnicas particulares de cada red puedan ser ignoradas al diseñar las aplicaciones que utilizarán los usuarios de los servicios.

Los dispositivos de interconexión de redes sirven para superar las limitaciones físicas de los elementos básicos de una red, extendiendo las topologías de esta.

Algunas de las ventajas que plantea la interconexión de redes de datos, son:

- Compartición de recursos dispersos.
- Coordinación de tareas de diversos grupos de trabajo.
- Reducción de costos, al utilizar recursos de otras redes.
- Aumento de la cobertura geográfica.

2.1.3.5.1 Tipos de Interconexión de redes.

Se pueden distinguir dos tipos de interconexión de redes, dependiendo del ámbito de aplicación:

- Interconexión de Área Local (LAN)
- Una interconexión de Área Local conecta redes que están geográficamente cerca, como puede ser la interconexión de redes de un mismo edificio o entre

edificios, creando una Red de Área Metropolitana (MAN, Metro Area Network,)

- Interconexión de Área Extensa (LAN con MAN y LAN con WAN)

La interconexión de Área Extensa conecta redes geográficamente dispersas, por ejemplo, redes situadas en diferentes ciudades o países creando una Red de Área Extensa (WAN, Wireless Area Networks)

2.1.3.5.2 Dispositivos de interconexión en las redes.

Cable

Al momento de elegir el cable a utilizar es importante considerar lo siguiente:

- Cuántos equipos hay que conectar
- Su distribución física: La distancia que los separa, si están en el mismo edificio o en varios.
- El ancho de banda que se necesite.
- La existencia de redes ya montadas o de equipos con tarjetas de red aprovechables.
- Las condiciones ambientales de los edificios: temperaturas, humedad, etc.
- Si hay que conectar pocos PCs en una misma oficina se podrá hacer con un cable coaxial, mientras que si se desea interconectar muchos equipos en espacios diferentes habrá que decidir por un cableado estructurado con UTP o con fibra óptica, en los casos en que las interferencias externas o las necesidades de ancho de banda la requiera.

El cable UTP está compuesto por cuatro pares de hilos trenzados, individualmente y entre ellos con un ciclo de trenzado de menos de 38 mm. El hilo usado es de 0'5 mm y está indicado para ser utilizado a temperaturas entre - 10ºC a 60ºC. Los colores con los que se identifican cada uno de los pares son:

- Par 1: Blanco-Azul/Azul
- Par 2: Blanco-Naranja/Naranja
- Par 3: Blanco-Verde/Verde

- Par 4: Blanco-Café/Café

El cable UTP se clasifica en categorías, dependiendo de la velocidad máxima que pueda soportar.

Patch Panel

Son estructuras metálicas con placas de circuitos que permiten interconexión entre equipos. Un Patch-Panel posee una determinada cantidad de puertos (RJ-45 End-Plug), donde cada puerto se asocia a una placa de circuito, la cual a su vez se propaga en pequeños conectores de cerdas (o dientes - mencionados con anterioridad).

En estos conectores es donde se ponchan las cerdas de los cables provenientes de los cajetines u otros Patch-Panels. La idea del Patch-Panel además de seguir estándares de redes, es la de estructurar o manejar los cables que interconectan equipos en una red, de una mejor manera. Para ponchar las cerdas de un cable Twisted Pair en el Patch-Panel se usa una ponchadora al igual que en los cajetines.

El estándar para el uso de Patch-Panels y Cables es el siguiente:

- Se conecta un cable o RJ-45 (Plug-End) de una maquina al puerto (Jack-End) del cajetín. Se debe tener cuidado con esto ya que el cable puede ser cruzado o no.
- De la parte dentada interna del cajetín se conectan las cerdas de otro cable hasta la parte dentada del Patch-Panel. El cable se pasa a través de las canaletas previamente colocadas.
- Del puerto externo del patch-panel (Jack-End) se coloca un cable corto hacia el hub o el Switch.

Conectores

Los conectores usados son los RJ45 macho y se los usará para la construcción de los patch cord de conexión externa de todos los dispositivos. Es importante saber que en el mercado existen conectores de varias calidades y que en muchos casos,

un mal contacto producido por un mal conector, puede bajar el rendimiento de una LAN.

Faceplates

Las placas toma datos o faceplates deberán ser de material termoplástico con 45° de inclinación, debe incluir 2 puertos (uno para datos y otro para voz), el color debe cumplir las normas de cableado para data y voz. El cual debe incluir dos biseles para colocar etiquetas que permitan identificar al usuario en forma instantánea. Debe contar con una aprobación UL. , debe contener los jack modulares montado.

Swicth

Un switch se describe a veces como un puente multipuerto. Mientras que un puente típico puede tener sólo dos puertos que enlacen dos segmentos de red, el switch puede tener varios puertos, según la cantidad de segmentos de red que sea necesario conectar.

Al igual que los puentes, los switchs aprenden determinada información sobre los paquetes de datos que se reciben de los distintos computadores de la red. Los switchs utilizan esa información para crear tablas de envío para determinar el destino de los datos que se están mandando de un computador a otro de la red.

Aunque hay algunas similitudes entre los dos, un switch es un dispositivo más sofisticado que un puente. Un puente determina si se debe enviar una trama al otro segmento de red, basándose en la dirección MAC destino.

Un switch tiene muchos puertos con muchos segmentos de red conectados a ellos. El switch elige el puerto al cual el dispositivo o estación de trabajo destino está conectado. Los switchs Ethernet están llegando a ser soluciones para conectividad de uso difundido porque, al igual que los puentes, los switchs mejoran el rendimiento de la red al mejorar la velocidad y el ancho de banda.

La conmutación es una tecnología que alivia la congestión en las LAN Ethernet, reduciendo el tráfico y aumentando el ancho de banda. Los switchs pueden remplazar a los hubs con facilidad debido a que ellos funcionan con las

infraestructuras de cableado existentes. Esto mejora el rendimiento con un mínimo de intrusión en la red ya existente.

Actualmente en la comunicación de datos, todos los equipos de conmutación realizan dos operaciones básicas: La primera operación se llama conmutación de las tramas de datos. La conmutación de las tramas de datos es el procedimiento mediante el cual una trama se recibe en un medio de entrada y luego se transmite a un medio de salida. El segundo es el mantenimiento de operaciones de conmutación cuando los switch crean y mantienen tablas de conmutación.

Los switchs operan a velocidades mucho más altas que los puentes y pueden admitir nuevas funcionalidades como, por ejemplo, las LAN virtuales.

Ventajas

- Un switch para Ethernet permite que varios usuarios puedan comunicarse en paralelo usando circuitos virtuales y segmentos de red dedicados en un entorno virtualmente sin colisiones. Esto aumenta al máximo el ancho de banda disponible en el medio compartido.
- Al desplazarse a un entorno de LAN conmutado es muy económico ya que el hardware y el cableado se pueden volver a utilizar.

2.1.3.6 Tendencias tecnológicas y seguridad.

Las principales tendencias del mercado de sistemas de información son las interconexiones de redes y destacan las siguientes:

- Tendencias de encaminamiento.

El mercado está en expansión, cada vez hay más ofertas de productos y además estos incorporan nuevas facilidades de encaminamiento. Tanto los fabricantes de concentradores como los de multiplexores están incorporando en sus productos capacidades de encaminamiento, unos con redes de área metropolitana y extensa, y otros incorporando facilidades de interconexión de LANs pero siempre ayudando a tener mayor control de la red y asegurar la información del usuario.

- Equipos de interconexión a bajo costo.

Los fabricantes están presentando equipos de bajo coste que permiten la interconexión de dependencias remotas. Las soluciones de encaminamiento son de diversos tipos: integradas en servidores de red, en concentradores, en pequeños equipos router, etc. Todos estos productos son fáciles de gestionar, operar y mantener y de buena confiabilidad y seguridad.

- Routers multiprotocolo.

Estos dispositivos han permitido a los usuarios transportar protocolos diferentes sobre la misma infraestructura de red, lo cual permitiría ahorrar en costes de la infraestructura de transmisión y una potencial mejora en la seguridad de los datos.

- Interconexión de LAN/WAN bajo Switchs.

Los conmutadores han evolucionado rápidamente dotándose de altas capacidades y velocidad de proceso. Pensados para soportar conmutación ATM (Asynchronous Transfer Mode, Modo de Transferencia Asíncrono) bajo una arquitectura punto a punto, han logrado gran implantación como mecanismo de interconexión de redes de área local heterogénea, Token Ring y Ethernet en un mismo dominio. Esto se consigue dado que el conmutador permite la segmentación de la red en subredes conectadas a cada uno de sus puertos que puede gestionar de manera independiente.
En la auditoria de seguridad informática se tomaran en cuenta las normas y aplicaciones que se deben realizar a cada unos de los componentes de red que se mencionan y por ende para una mejor administración y servicio que se preste se debe aplicar las especificaciones mencionadas cuyo objetivo es de precautelar la correcta conexión de cada uno de los nodos en los diferentes backbone de los edificios de la UNEMI.

Capacidad de gestión.
Los fabricantes están dotando a sus dispositivos de interconexión con mayores capacidades de gestión que permitan la monitorización de la red mediante

estaciones de gestión y control de los dispositivos de la red, enviando comandos por la red desde la estación de gestión hasta el dispositivo de la red para cambiar o inicializar su configuración.

2.2. Marco conceptual.

Proceso.-

Un Proceso consiste en transformar entradas (insumos) en salidas, (bienes y/o servicios) por medio del uso de recursos físicos, tecnológicos, humanos, controlando la seguridad de la información.

Un proceso productivo incluye acciones que ocurren en forma planificada, y producen un cambio o transformación de materiales, objetos y/o sistemas, al final de los cuales obtenemos un producto.

Infraestructura.-

Se denomina infraestructura aquella realización humana diseñada y dirigida por profesionales de arquitectura, ingeniería civil, etc. que sirven de soporte para el desarrollo de otras actividades y su funcionamiento, necesario en la organización.

Influencia.-

La influencia puede ser coercitiva, atractiva, cooperativa o competitiva y se da generalmente en tres formas:

- Político-estratégica, a través del uso o amenaza de uso de la fuerza.
- Diplomática, por grupo de poder o cabildeos (lobbies), negociaciones, etc.
- Económica, mediante bloqueos, boicots, etc.

Comunicación entre oficina.-

La comunicación por medio de una red se lleva a cabo en dos diferentes categorías: la capa física y la capa lógica.

La capa física incluye todos los elementos de los que hace uso un equipo para comunicarse con otros equipos dentro de la red, como, por ejemplo, las tarjetas de red, los cables, las antenas, etc.

Descripciones de las capas lógicas.

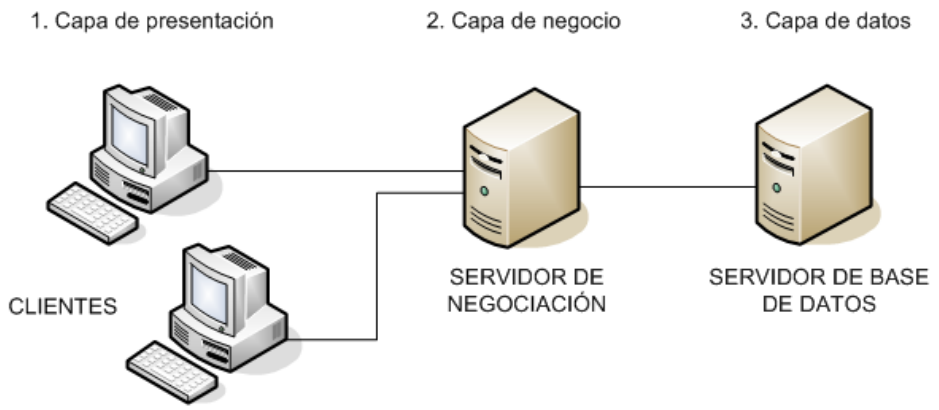


Gráfico 2: Capas lógicas.

- **Capa de presentación**. La capa de presentación está formada por la lógica de aplicación, que prepara datos para su envío a la capa de cliente y procesa solicitudes desde la capa de cliente para su envío a la lógica de negocios del servidor.

- **Capa de servicios de negocios**. La capa de servicios de negocio consiste en la lógica que realiza las funciones principales de la aplicación: procesamiento de datos, implementación de funciones de negocios, coordinación de varios usuarios y administración de recursos externos como, por ejemplo, bases de datos o sistemas heredados.
- **Capa de datos**. La capa de datos está formada por los servicios que proporcionan los datos persistentes utilizados por la lógica de negocios.
  Los datos pueden ser datos de aplicaciones almacenados en un sistema de administración de bases de datos o pueden incluir información de recursos y

directorios almacenada en un almacén de datos de protocolo ligero de acceso a directorios (LDAP).

Los servicios de datos también pueden incluir alimentación de datos de orígenes externos o datos a los que se puede obtener acceso desde sistemas informáticos heredados.

Descripción general del diseño de la red.

Se requieren diferentes tipos de dispositivos para la red alámbrica e inalámbrica de la universidad.

La siguiente tabla incluye los dispositivos principales que se requieren así como su uso, finalidad y desafíos relacionados.

Tabla 2: Diseño de red.

Servicio	**Dispositivo principal**	**Uso principal**	**Beneficios**	**Desafío**
Red de área local (LAN) alámbrica	Conmutadores	Conectar servidores, dispositivos y PCs	Conectividad LAN de alta velocidad	Cablear la LAN
Conectividad alámbrica segura en la LAN	Puntos de acceso alámbricos (APs)	Conectar dispositivos habilitados de manera inalámbrica (tales como PCs portátiles, Tablet PCs y PDAs)	Movilidad del usuario	Seguridad Velocidad de la transmisión
Conexión segura a Internet	Firewall	Proporcionar acceso de entrada y salida a Internet	Conectarse con los servidores	Seguridad

Gráfico 3: Grafico conectividad entre edificios.

Topología de la red.

La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios.

La otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos. Las topologías generalmente utilizadas son las siguientes:

Topologías físicas.

- Una topología de bus circular usa un solo cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este backbone.
- La topología de anillo conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.
- La topología en estrella conecta todos los cables con un punto central de concentración.

- Una topología en estrella extendida conecta estrellas individuales entre sí mediante la conexión de hubs o switchs. Esta topología puede extender el alcance y la cobertura de la red.
- Una topología jerárquica es similar a una estrella extendida. Pero en lugar de conectar los hubs o switchs entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.
- La topología de malla se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio. El uso de una topología de malla en los sistemas de control en red de una planta nuclear sería un ejemplo excelente.
- Como se puede observar en el gráfico, cada host tiene sus propias conexiones con los demás hosts. Aunque Internet cuenta con múltiples rutas hacia cualquier ubicación, no adopta la topología de malla completa.

También hay otra topología denominada árbol.

Topologías lógicas.

La topología lógica de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast y transmisión de tokens.

- La topología broadcast simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. No existe una orden que las estaciones deban seguir para utilizar la red. Es por orden de llegada, es como funciona Ethernet.
- La topología transmisión de tokens controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial. Cuando un host recibe el token, ese host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token al siguiente host y el proceso se vuelve a repetir. Dos ejemplos de redes que utilizan la transmisión de tokens son Token Ring y la Interfaz de datos distribuida por fibra (FDDI). Arcnet es una variación de Token Ring y FDDI. Arcnet es la transmisión de tokens en una topología de bus.

Tipos.

La oferta de redes de área local es muy amplia, existiendo soluciones casi para cualquier circunstancia. Podemos seleccionar el tipo de cable, la topología e incluso el tipo de transmisión que más se adapte a nuestras necesidades. Sin embargo, de toda esta oferta las soluciones más extendidas son tres: Ethernet, Token Ring y Arcnet.

Componentes de la red

- **Servidor:** el servidor es aquel o aquellos ordenadores que van a compartir sus recursos hardware y software con los demás equipos de la red. Sus características son potencia de cálculo, importancia de la información que almacena y conexión con recursos que se desean compartir.

- **Estación de trabajo**: los ordenadores que toman el papel de estaciones de trabajo aprovechan o tienen a su disposición los recursos que ofrece la red así como los servicios que proporcionan los Servidores a los cuales pueden acceder.

- **Gateways o pasarelas:** es un hardware y software que permite las comunicaciones entre la red local y grandes ordenadores (mainframes). El gateway adapta los protocolos de comunicación del mainframe (X25, SNA, etc.) a los de la red, y viceversa.

- **Bridges o puentes**: es un hardware y software que permite que se conecten dos redes locales entre sí. Un puente interno es el que se instala en un servidor de la red, y un puente externo es el que se hace sobre una estación de trabajo de la misma red. Los puentes también pueden ser locales o remotos. Los puentes locales son los que conectan a redes de un mismo edificio, usando tanto conexiones internas como externas. Los puentes remotos conectan redes distintas entre sí, llevando a cabo la conexión a través de redes públicas, como la red telefónica, RDSI o red de conmutación de paquetes.

- **Tarjeta de red**: también se denominan NIC (Network Interface Card). Básicamente realiza la función de intermediario entre el ordenador y la red de comunicación. En ella se encuentran grabados los protocolos de comunicación de la red. La comunicación con el ordenador se realiza normalmente a través de las ranuras de expansión que éste dispone, ya sea ISA, PCI o PCMCIA. Aunque algunos equipos disponen de este adaptador integrado directamente en la placa base.

- **El medio**: constituido por el cableado y los conectores que enlazan los componentes de la red. Los medios físicos más utilizados son el cable de par trenzado, par de cable, cable coaxial y la fibra óptica (cada vez en más uso esta última).

- **Concentradores de cableado**: una LAN en bus usa solamente tarjetas de red en las estaciones y cableado coaxial para interconectarlas, además de los conectores, sin embargo este método complica el mantenimiento de la red ya que si falla alguna conexión toda la red deja de funcionar. Para impedir estos problemas las redes de área local usan concentradores de cableado para realizar las conexiones de las estaciones, en vez de distribuir las conexiones el concentrador las centraliza en un único dispositivo manteniendo indicadores luminosos de su estado e impidiendo que una de ellas pueda hacer fallar toda la red.

Existen dos tipos de concentradores de cableado:

1. Concentradores pasivos: actúan como un simple concentrador cuya función principal consiste en interconectar toda la red.
2. Concentradores activos: además de su función básica de concentrador también amplifican y regeneran las señales recibidas antes de ser enviadas.

Los concentradores de cableado tienen dos tipos de conexiones: para las estaciones y para unirse a otros concentradores y así aumentar el tamaño de la red. Los concentradores de cableado se clasifican dependiendo de la manera en que internamente realizan las conexiones y distribuyen los mensajes. A esta característica se le llama topología lógica.

Existen dos tipos principales:

1. Concentradores con topología lógica en bus (HUB): estos dispositivos hacen que la red se comporte como un bus enviando las señales que les llegan por todas las salidas conectadas.
2. Concentradores con topología lógica en anillo (MAU): se comportan como si la red fuera un anillo enviando la señal que les llega por un puerto al siguiente.

Desempeño Laboral.

Es un procedimiento estructural y sistemático para medir, evaluar e influir sobre los atributos, comportamientos y resultados relacionados con el trabajo, así como el grado de ausentismo, con el fin de descubrir en qué medida es productivo el empleado y si podrá mejorar su rendimiento futuro.

Planificación.

La planificación se refiere a las acciones llevadas a cabo para realizar planes y proyectos de diferente índole.

Desconocimiento de tecnologías de Red.

La tecnología siempre ha formado parte del ser humano y de su desarrollo. Las primeras tecnologías del ser humano eran simples piedras. Éstas, transformadas y utilizadas adecuadamente, se utilizaban como herramientas para diferentes labores como cortar, cazar o manipular otros instrumentos. La propia definición de tecnología dice que se trata del conjunto de saberes que permiten fabricar objetos y modificar el medio ambiente, incluyendo las plantas y animales, para satisfacer las necesidades y deseos humanos.

Telecomunicaciones e Internet.

Telecomunicación es toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos, datos o información de cualquier naturaleza realizada por el hombre, por hilo, radioelectricidad.

Las telecomunicaciones pueden verse como un conjunto de medios que permiten el enlace de dos puntos que se encuentran a una distancia considerable, utilizando para ello y según el caso, diferentes dispositivos que varían desde un simple aparato telefónico hasta los servicios de comunicación vía satélite.

Los computadores sobrepasan sus roles tradicionales como simples herramientas de procesamientos de texto, para convertirse en herramientas de procesamiento y transmisión de información. Como herramienta de comunicación, los computadores minimizan las barreras de tiempo y espacio, mediante los medios propios de las telecomunicaciones.

El crecimiento de los servicios de telecomunicaciones es evidente al observar avances como el sistema de radio móvil celular planeado y parcialmente instalado alrededor del mundo y el reciente énfasis en los sistemas de transmisión local, nacional o internacional utilizando fibra óptica.

El propósito de los sistemas de comunicación es proveer los medios necesarios para facilitar la comunicación entre personas, empresas, instituciones educativas y otras, siendo de vital importancia, dado el gran volumen de información que se necesita manejar en la actualidad.

Internet.

En principio, es una red de redes. Una red significa dos o más computadoras conectadas entre sí. Las razones más importantes para crear una red son:

- Permitir a las personas comunicarse
- Compartir recursos

Sin embargo, Internet es mucho más que un gran conjunto de redes de computadoras interconectadas. Es la posibilidad de que millones de personas en el mundo se comuniquen entre si y compartan sus conocimientos e información.

Es una gran sociedad orientada a los humanos y que en términos generales ha servido para bien.

Desde sus inicios Internet ofreció una serie de servicios tales como:

- Correo electrónico
- Conexión remota computadora a computadora
- Servicio finger
- Usenet
- FTP anónimo
- Utilería Talk
- Servidores Archie
- Gopher
- Servidores Wais
- BBS
- World Wide Web (www)

En la actualidad algunos de los servicios citados ya no se utilizan. De los servicios anteriores, principalmente dos han permanecido: el correo electrónico y la World Wide Web, mejor conocida como la Web.

La Web comenzó siendo un proyecto del Laboratorio Europeo de Física de Partículas en Suiza. Está basada en el concepto de hipertexto y ha sido uno de los mejores recursos para navegar por Internet. En la web se muestra la información organizada en páginas de documentos de hipertexto.

La concepción original del hipertexto consistía en un texto con algunas palabras seleccionadas que se podían “expandir” en más información relacionada con esas palabras. A esta posibilidad se le llamó liga o vínculo. En la actualidad las páginas de la Web ofrecen las ligas de navegación tanto en palabras seleccionadas de un texto como en áreas sensibles de la página u otros objetos como botones y gráficos. Las páginas incluso pueden contener elementos animados.

Internet fue posible gracias al desarrollo de las telecomunicaciones mundiales. Desde la comunicación satelital, hasta el componente más elemental en los equipos modernos que permiten enlaces rápidos, limpios y seguros. La televisión como

medio de comunicación masiva ha sabido aprovechar también estos recursos, haciendo la transmisión de imágenes de los hechos en el mismo instante de su ocurrencia.

La digitalización y los medios de almacenamiento digital han permitido grabar el conocimiento en espacios nunca antes imaginados, que combinados con las altísimas velocidades de procesamiento de los sistemas de cómputo y las posibilidades de transmisión de datos han dado origen al fenómeno que hemos llamado revolución de las tecnologías de la información.

2.3. Hipótesis y Variables.

2.3.1. Hipótesis General.

El no contar con una auditoria de seguridad informática confiable está influyendo en los procesos de servicio del departamento del TIC's de la Universidad Estatal de Milagro.

La realización de una auditoría de seguridad informática permite evaluar en qué condiciones esta la Seguridad Informática del Dpto. de Tecnologías de la UNEMI.

2.3.2. Hipótesis Particulares.

El acceso a lugares restringidos, mala utilización de software, y no aplicación de respaldos de información está influenciado por no contar con una auditoria de Seguridad Informática en el departamento del TIC's de la Universidad Estatal de Milagro.

La poca importancia que se da a la Seguridad Informática está ocasionando incertidumbre por manipulación o pérdida de la información almacenada en los equipos de cómputo.

El retraso de trabajo, en ocasiones es causado por no contar con una auditoria de políticas de Seguridad Informática sobre desastres informáticos en el departamento del TIC's de la Universidad Estatal de Milagro.

2.4. Variables.

Tabla 3: Variables Dependientes

DEPENDIENTES (efecto)	**Indicadores**	**Variables Empíricas**
Los procesos del departamento del TIC's de la Universidad Estatal de Milagro	Monitoreo de actividades	Proceso
Influencia por no contar con políticas y procedimientos de Seguridad Informática en el departamento del TIC's de la Universidad Estatal de Milagro	Monitoreo de actividades	Influencia
No contar con instructivo legal de Seguridad Informática en el departamento del TIC's de la Universidad Estatal de Milagro	Monitoreo de actividades	Influencia
Desempeño laboral de la Universidad Estatal de Milagro causado por no contar con políticas y procedimientos de Seguridad Informática	Evaluación del Desempeño	Desempeño Laboral
Estrategia para aplicar una auditoria de seguridad informática legal en el departamento del TIC's de la Universidad Estatal de Milagro	Encuestas Evaluación	Planificación

Tabla 4: Variables Independientes.

INDEPENDIENTES (causas)	**Indicadores**	**Variables Empíricas**
El desconocimiento de los beneficios de contar con un instructivo legal de Seguridad Informática en el departamento del TIC's de la Universidad Estatal de Milagro.	Test de conocimiento	Desconocimiento de Seguridad Informática
Perdida de información y poca restricciones a lugares de computo no permitidos	Evaluación Control	Perdida de Información
Desarrollo de una Seguridad Informática estructurada y confiable	Control Evaluación	Desarrollo

En la investigación realizada nos encontramos con variables de tipo cualitativo, mediante las cuales un grupo de individuos se clasifican en dos o más categoría.

Las proporciones son una forma habitual de expresar frecuencias cuando la variable objeto de estudio tiene dos posibles respuestas, como presentar o no un evento de interés (rentabilidad, comercialización, beneficio social, etc.).

Cuando lo que se pretende es comparar dos o más grupos de sujetos con respecto a una variable categórica, los resultados se suelen presentar a modo de tablas de doble entrada que reciben el nombre de tablas de contingencia.
Así, la situación más simple de comparación entre dos variables cualitativas es aquella en la que ambas tienen sólo dos posibles opciones de respuesta (es decir, variables dicotómicas).

En esta situación la tabla de contingencia se reduce a una tabla dos por dos como la que se muestra en la siguiente tabla.

Tabla 5: Tabla de contingencia general para la comparación de dos variables.

	Factor A		
Factor B	**Presente**	**Ausente**	**Total**
Presenta	A	B	a + b
Ausente	C	D	c + d
Total	a + c	b + d	N

Supongamos que se quiere estudiar la posible asociación entre el hecho de que una Institución cuenta con políticas de seguridad informática y la percepción de confianza en los usuarios de la UNEMI. Por lo tanto, se trata de ver que Instituciones con políticas de seguridad informática tuvo una mayor confianza en los servicios suministrados o no y que Institución sin políticas de seguridad informática tuvo mayor confianza en los servicios suministrados o no.

Para responder a esta pregunta se realiza un estudio comparativo en 11 Instituciones Públicas en el cantón de Milagro. Los resultados de este estudio se muestran en la siguiente Tabla.

Tabla 6: Tabla contingencia Confianza en los usuarios con o sin la aplicación de políticas de seguridad informática.

	Factor 1: Confianza en los usuarios			
		Presente	**Ausente**	**Total**
Factor 2:	**Presente**	5	1	6
Aplican Políticas de Seguridad Informática.	**Ausente**	1	4	5
	Total	6	5	11

En la Tabla 6, a, b, c y d son las frecuencias observadas del suceso en la realidad de nuestro ejemplo de estudio (5, 1, 1 y 4), siendo n (11) el número total de casos estudiados, y a+b, c+d, a+c y b+d los totales marginales.

En el análisis, a+b=4 sería el número Instituciones con Políticas de Seguridad Informática, c+d=3 el número total de Instituciones sin Políticas de Seguridad Informática, a+c=4 con crecimiento económico y b+d=3 sin crecimiento económico.

Ante una tabla de contingencia como la anterior pueden planteársenos distintas cuestiones. En primer lugar, se querrá determinar si existe una relación estadísticamente significativa entre las variables estudiadas. En segundo lugar, nos interesará cuantificar dicha relación y estudiar su relevancia rentable. Esta última cuestión podrá resolverse mediante las denominadas medidas de asociación o de efecto (riesgo relativo (RR), odds ratio (OR), reducción absoluta del riesgo (RAR)).

Por otro lado, para responder a la primera pregunta, la metodología de análisis de las tablas de contingencia dependerá de varios aspectos como son: el número de categorías de las variables a comparar, del hecho de que las categorías estén ordenadas o no, del número de grupos independientes de sujetos que se estén considerando o de la pregunta a la que se desea responder.

Existen diferentes procedimientos estadísticos para el análisis de las tablas de contingencia como la prueba χ^2, la prueba exacta de Fisher, la prueba de McNemar o la prueba Q de Cochran, entre otras. Aquí se expondrá el cálculo e interpretación de la prueba χ^2 como método estándar de análisis en el caso de grupos independientes.

La prueba χ^2 en el contraste de independencia de variables aleatorias cualitativas.

La prueba χ^2 permite determinar si dos variables cualitativas están o no asociadas. Si al final del estudio concluimos que las variables no están relacionadas podremos decir con un determinado nivel de confianza, previamente fijado, que ambas son independientes.

Para su cómputo es necesario calcular las frecuencias esperadas (aquellas que deberían haberse observado si la hipótesis de independencia fuese cierta), y compararlas con las frecuencias observadas en la realidad.

De modo general, para una tabla r x k (r filas y k columnas), se calcula el valor del estadístico χ^2 como sigue:

$$\chi^2 = \sum_{i=1}^{r}\sum_{j=1}^{k}\frac{\left(O_{ij} - E_{ij}\right)^2}{E_{ij}}$$

Donde:

O_{ij} denota a las frecuencias observadas. Es el número de casos observados clasificados en la fila i de la columna j.

E_{ij} denota a las frecuencias esperadas o teóricas. Es el número de casos esperados correspondientes a cada fila y columna. Se puede definir como aquella frecuencia que se observaría si ambas variables fuesen independientes.

Así, el estadístico χ^2 mide la diferencia entre el valor que debiera resultar si las dos variables fuesen independientes y el que se ha observado en la realidad. Cuanto mayor sea esa diferencia (y, por lo tanto, el valor del estadístico), mayor será la relación entre ambas variables. El hecho de que las diferencias entre los valores observados y esperados estén elevadas al cuadrado en (1) convierte cualquier diferencia en positiva. El test χ^2 es así un test no dirigido (test de planteamiento bilateral), que nos indica si existe o no relación entre dos factores pero no en qué sentido se produce tal asociación.

Para obtener los valores esperados E_{ij}, estos se calculan a través del producto de los totales marginales dividido por el número total de casos (n). Para el caso más sencillo de una tabla 2x2 como la Tabla 1, se tiene que:

$$E_{11} = \frac{(a+b)\times(a+c)}{n} \qquad E_{21} = \frac{(c+d)\times(a+c)}{n}$$

$$E_{12} = \frac{(a+b)\times(b+d)}{n} \qquad E_{22} = \frac{(c+d)\times(b+d)}{n}$$

Para los datos del ejemplo en la Tabla 2 los valores esperados se calcularían como sigue:

$E_{11} = \frac{6 \times 6}{11} = 3{,}272$ $\qquad$ $E_{21} = \frac{5 \times 6}{11} = 2{,}727$

$E_{12} = \frac{6 \times 5}{11} = 2{,}727$ $\qquad$ $E_{22} = \frac{5 \times 5}{11} = 2{,}272$

De modo que los valores observados y esperados para los datos del ejemplo planteado se muestran en la siguiente Tabla.

Tabla 7: Tabla contingencia crecimiento económico con Políticas de Seguridad Informática.

	Factor 1:	**Crecimiento Económico**		
		Presente	**Ausente**	**Total**
Factor 2:	**Presente**	5(3,272)	1(2,727)	6
Políticas de Seguridad Informática	**Ausente**	1(2,727)	4(2,272)	5
	Total	6	5	11

El valor del estadístico χ^2, para este ejemplo en concreto, vendría dado entonces como:

$$X^2 = \frac{(5-3{,}272)^2}{3{,}272} + \frac{(1-2{,}727)^2}{2{,}727} + \frac{(1-2{,}727)^2}{2{,}727} + \frac{(4-2{,}272)^2}{2{,}272} = 4{,}414$$

p = 0,04

Dado este valor, que se aproxima a cero, en el nivel de significancia, la hipótesis se confirma.

Formula en Excel DISTR.CHI (4,41; Grados de libertad en este caso)

A la vista de este resultado, lo que tenemos que hacer ahora es plantear un contraste de hipótesis entre la hipótesis nula:

H0: No hay asociación entre las variables, es decir hay menor o no hay crecimiento económico al no tener una política de sistema de información..

Y la hipótesis alternativa:

Ha: Sí hay asociación entre las variables, es decir hay mayor crecimiento económico al tener una política de sistema de información

Bajo la hipótesis nula de independencia, se sabe que los valores del estadístico χ^2 se distribuyen según una distribución conocida denominada ji-cuadrado, que depende de un parámetro llamado “grados de libertad” (g.l.). Para el caso de una tabla de contingencia de r filas y k columnas, los g.l. son igual al producto del número de filas menos 1 (r-1) por el número de columnas menos 1 (k-1).

De ser cierta la hipótesis nula, el valor obtenido debería estar dentro del rango de mayor probabilidad según la distribución ji-cuadrado correspondiente.

El valor-p que usualmente reportan la mayoría de paquetes estadísticos no es más que la probabilidad de obtener, según esa distribución, un dato más extremo que el que proporciona el test o, equivalentemente, la probabilidad de obtener los datos observados si fuese cierta la hipótesis de independencia.

Si el valor-p es muy pequeño (usualmente se considera $p<0.05$) es poco probable que se cumpla la hipótesis nula y se debería de rechazar.

CAPÍTULO III
MARCO METODOLÓGICO

3.1 Tipo, diseño y perspectiva de la investigación.

La investigación aplicada de forma factible; según su objetivo gnoseológico es correlacional, descriptivo, explicativo; además según su contexto es de campo y se desarrollará desde una perspectiva cuantitativa y cualitativa de forma longitudinal.

Para el estudio la investigación es:

1. Aplicada, ya que depende de sus descubrimientos y aportes teóricos y busca confrontar la teoría a la realidad.
2. Correlacional, siendo la medición y evaluación en relación de las variables.
3. Descriptivo, tiene como propósito la descripción de eventos y situaciones representativas de la unidad de análisis específica.
4. Explicativo, va más allá de la descripción de los conceptos dirigidos con la finalidad de responder las causas de los eventos, estableciendo porqué ocurre el fenómeno.
5. De campo, porque el trabajo de investigación se lo efectuará de manera natural.
6. Bajo la fundamentación cuantitativa, para obtener respuestas concretas y cuantificables por parte de una muestra representativa de la población ante el problema de investigación.
7. Cualitativa, estableciendo una correlación de variables que comprende las razones y motivaciones subyacentes de las actitudes, preferencias o comportamientos de las personas ante el trabajo de investigación.
8. Cuantitativa, antecede a la recolección de datos y consiste en la definición de los pasos que se seguirán desde la elección del problema hasta el diseño metodológico.

Se divide en tres fases principales:

- La primera define qué es lo que se investigará,
- La segunda se establece cuál es la base teórica del problema y
- La tercera se determina cómo se investigará el problema.

3.2 Población y muestra.

En el trabajo de investigación, el universo está integrado, como se describe en la tabla 8, anexa en la siguiente página, por los siguientes elementos:

Tabla 8: MARCO MUESTRAL: Numero de personal involucrado con los servicios de Tecnología de los Departamentos y Unidades Académicas de la UNEMI

Ubicación del Departamento	Número de personal
Recursos Humanos Bloque “C”	7
Administrativo Bloque “C” “G”	16
Bienestar Universitario Bloque “B”	8
Ingles Bloque “B”	5
Admisión Bloque “B”	4
Obras Universitaria Bloque “B”	3
Investigación Bloque “C”	10
Evaluación Bloque “C”	5
Conducción Bloque “D”	3
Post grado	7
Ciencia de la Educación Bloque “F”	6
CSIA Bloque “H” y Bloque “P”	10
Ciencia Salud Bloque “L”	6
Biblioteca Bloque “M”	3
Vicerrectorado Adm./ Acad. Bloque “M”	3
ODI Bloque “M”	7
Relaciones Publicas Bloque “M”	4
Ciencias Administrativas Bloque “O”	9
Rectorado Bloque “R”	7
TIC’s Bloque “R”	13
Secretaria General Bloque “R”	3
Auditoria Bloque “R”	3
Financiero Bloque “R”	15
Asesoría Legal Bloque “R”	2
Educación continua Bloque “S”	7
Ciencias Ingeniería Bloque “T”	8
Docente Aulas Clase	104
Total Personal	**288**

Fuente: Dpto. Tecnologías y RR. HH Marzo. 2012.

El estudio que se ha realizado, está dirigido a todas la áreas que tienen que ver con el departamento del TIC's y que utilizan los sistemas informáticos, correo e internet.
El universo en estudio, lo constituye los 288 empleados que están involucrados con los servicios del departamento del TIC's.

Parámetros muéstrales

El Marco Muestral utilizado en el diseño de la muestra corresponde a la totalidad área o departamentos de la UNEMI que utilizan los servicios informáticos del departamento del TIC's, por lo tanto el muestreo será por cuotas y dirigido, a la unidad final de muestreo: El administrador o quien lo represente de cada departamento, de manera tal que los instrumentos de interés estén en los parámetros representados apropiadamente.

Tamaño de la muestra

Para establecer el tamaño de la muestra la calcularemos mediante la siguiente expresión matemática de manera probabilística:

$$n = \frac{Z^2PQN}{(N-1)\frac{E^2}{K^2} + Z^2PQ}$$

De donde:

Tabla 9: Simbología:

n	Tamaño de la muestra.
PQ	Constante de la varianza de la población (0.50)
N	Tamaño de la población.
E^2	Error máximo admisible (al 1% = 0.01; 2 % = 0.02; 3% = 0.03, etc.)
	A mayor error probable, menor tamaño de la muestra y viceversa.
K^2	Coeficiente de corrección del error. (2)

Usuarios que utilizan los servicios básicos del departamento del TIC's son 288

$$N = \frac{(1{,}96*1{,}96)*(0{,}5*0{,}5) \quad * \quad 288}{(288-1)* \quad \frac{0.005}{2} \quad + \quad (1{,}96*1{,}96)*(0{,}5*0{,}5)}$$

$$N = \frac{276{,}5952}{1{,}6779} = \mathbf{165}$$

165 empleados de la UNEMI corresponden a la muestra de los seleccionados al azar.

3.3 Métodos de investigación.

3.3.1 Método teórico.

3.3.1.1 Método histórico – lógico.

Determina los antecedentes históricos de la evolución del proceso de análisis, diseño. Implementación y evaluación de la tecnología y su incidencia de forma cronológica; y el conocer la evolución y desarrollo por lo que se hace necesario revelar su origen y las etapas del desenvolvimiento técnico de los sistemas y la planificación desde sus inicios.

3.3.1.2 Método analítico –sintético.

El método analítico-sintético para obtener la caracterización del proceso integral universitario y su intervención de todos sistemas de la comunidad institucional.

Igualmente para procesar la información que se pretende analizar y obtener información real.

3.3.1.3 Método inductivo – deductivo.

Inicia los casos, hechos o fenómenos particulares para llegar al descubrimiento de un principio o ley general que rige, es decir, va de lo particular a lo general por medio del análisis; pero el método deductivo parte de leyes generales y de estas consecuencias se aplican a casos particulares; es decir va de lo general a lo particular, por medio de la síntesis.

3.3.1.4 Método Hipotético – deductivo.

Se plantea la hipótesis que se puede analizar deductiva o inductivamente y posteriormente comprobar la incidencia del cumplimiento de la planificación a los proyectos informáticos como apoyo al desarrollo tecnológico de la seguridad informática del Dpto. Tecnologías de la UNEMI

3.3.2 Método Empírico.

3.3.2.1 Métodos empíricos fundamentales.

La observación se realizara de forma directa, estructurada y no oculta para establecer los eventos tal como ocurren, con respecto al reclutamiento y selección de personal en la UNEMI sin que afecten los hechos en su forma natural.

3.3.2.2 Métodos empíricos complementarios o técnicas.

- La conversación, para determinar los criterios del personal involucrado en el proceso de cumplimiento de los proyectos informáticos y su influencia en las actividades de la universidad y los efectos que provoca.
- La encuesta, para conocer el criterio del impacto de no cumplir con las planificaciones previstas y el conocer el criterio de resistencia a los nuevos ambientes tecnológicos.
- El criterio de expertos, para conocer la opinión de personal calificado.

3.4 Procesamiento de la información.

Para la investigación se utilizará como instrumento de medición un cuestionario estructurado, administrado, al cual se aplicara el método de la encuesta lo que permitirá medir los indicadores; y obtener información de la seguridad informática en el Departamento del TIC's objeto del estudio.

Se utilizará el paquete estadístico SPSS para ingresar los datos y proceder a sus análisis, utilizando cuadros estadísticos para representar los resultados obtenidos además de obtener un cruce de información de datos tabulados.

CAPÍTULO IV
ANÁLISIS DE LOS RESULTADOS

4.1 Análisis de la situación actual.

La Universidad Estatal de Milagro es el primer centro de educación superior ubicado en la ciudad de Milagro, tiene un departamento de Tecnologías que no posee en la actualidad políticas y procedimientos de seguridad informático que permitan salvaguardar la información que ahí se guarda de toda la institución, por lo que no se ha dado mucha importancia tener un plan de contingencias sobre algún desastre o perdida de información.

Esta falta de políticas y procedimientos para proteger la información de los sistemas de la universidad, impide tener confiabilidad de los datos que ahí se almacenan y se controla, entre las distintas oficinas o edificios de la institución, esto se traduce con cifras alarmantes para una actividad en el cual el no conocer o aplicar políticas de respaldo es vital por la importancia de los datos guardados y equipos informáticos.

De las entrevistas realizadas se encuentra que la mayoría del personal del TIC'S y Autoridades Universitarias no conocen de la existencia de plan de contingencias o políticas y procedimientos que proteja la información de toda la universidad. Lo que nos indica que hay un total desconocimiento de las leyes y responsabilidades que se tiene con los datos y equipos informáticos del sector público y que está normado bajo parámetros administrativos y penales como lo indica normas de control interno de bienes públicos según la Contraloría General del Estado. Por lo que debemos apegar la propuesta de auditar al departamento del TIC's, para mejoramiento de control de la información almacenada y procedimientos a seguir en casos de emergencias

4.2 Comparación, evaluación, tendencia y perspectiva.

Se considera para el desarrollo de esta encuesta la situación actual en la que se encuentra el departamento del TIC's y lo que los usuarios tienen conocimiento de cómo viene trabajando con los servicios que se presta a los empleados de la universidad, además se procedió a tabular los datos obtenidos utilizando el programa estadístico SPSS; se aplica el instrumento de medición de la investigación a las autoridades y empleados Universitarios, Directores, Coordinadores y Asesores Académicos, Jefes de Sección y Directores Departamentales y personal de apoyo un total de 165, las respuestas a las preguntas realizadas van a permitir establecer la propuesta de auditar el departamento del TIC's y verificar que es lo que están haciendo bien y que es lo que hay que mejorar para cumplir con sus objetivos y prestar servicios de calidad.

Es importante indicar que para conocer que visión tienen los empleados de la UNEMI sobre la confiabilidad en los servicios que ellos presta el departamento del TIC's a la comunidad universitaria y la seguridad informática que tienen, se procedió a realizar las siguientes preguntas.

Interpretación de datos.

Pregunta 1

¿Conoce usted que es una Auditoria de Sistemas de Información?

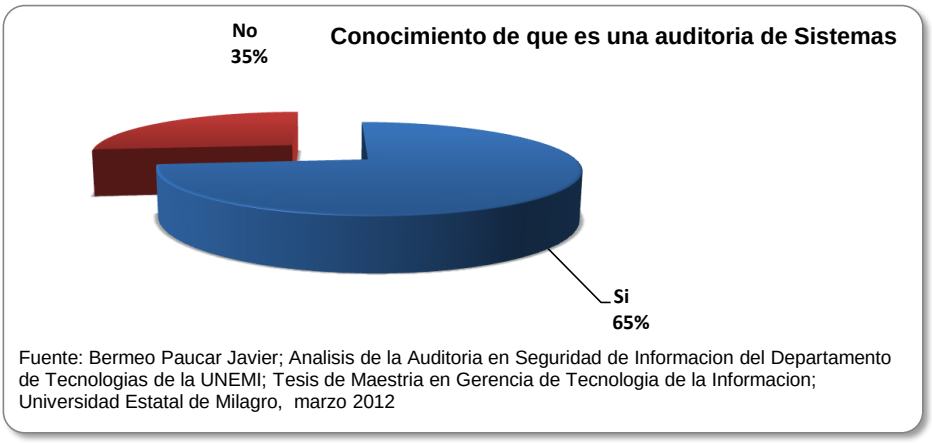


Gráfico 4: Conocimiento de que es una auditoria de sistemas

Análisis.

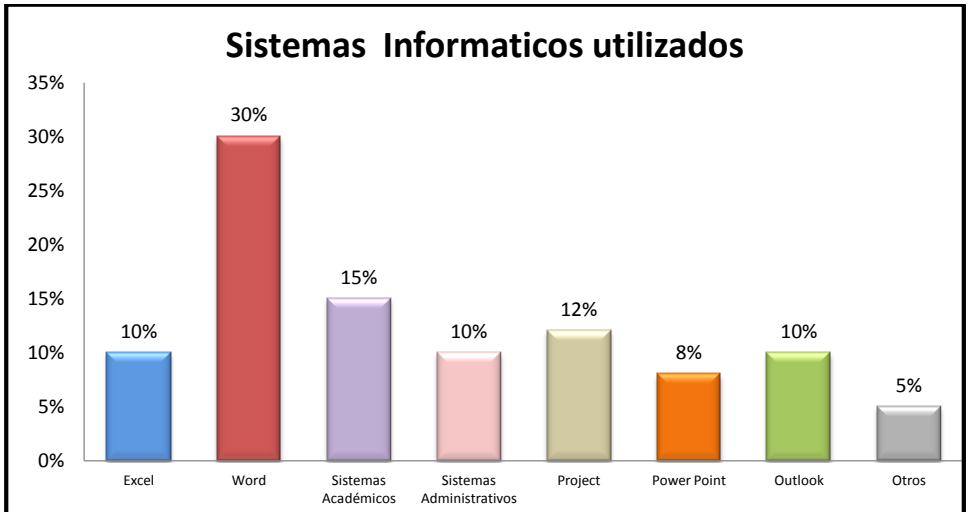
7 de cada 10 miembros de la comunidad de la Universidad Estatal de Milagro, desconocen que es una Auditoria de Sistemas de Información 65%, lo cual explica que el nivel de compromiso de los miembros de la institución tienen es un nivel de conocimiento básico de lo que es una auditoria de sistemas, por diferentes causas no ha rendido un resultado satisfactorio, por lo que se debería determinar las causantes, como la comunicación que se debe de establecer y la capacitación sobre el tema.

Conclusión.

Se puede indicar que no existe una difusión acertada de lo que es una auditoria de sistemas informáticos e indicar a cada uno de los usuarios que responsabilidad tienen cuando se ejecuta una acción como esta, por lo que se debe involucrar a todos los empleados a precautelar sus equipos y la información que tiene estos.

Pregunta 2

¿Qué sistemas informáticos, utiliza comúnmente para realizar sus labores de trabajo?



Fuente: Bermeo Paucar Javier; Analisis de la Auditoria en Seguridad de Informacion del Departamento de Tecnologias de la UNEMI; Tesis de Maestria en Gerencia de Tecnologia de la Informacion; Universidad Estatal de Milagro, marzo 2012

Gráfico 5: Sistemas informáticos que utilizan para su trabajo

Análisis.

Considerando que la herramienta más utilizada es el procesador de textos WORD (30%) y luego están los sistemas académicos y administrativos en un 25% sumados los dos, están conscientes de la importancia de aplicar una auditoria para saber que la información que guardan y consultan están correctamente almacenados.

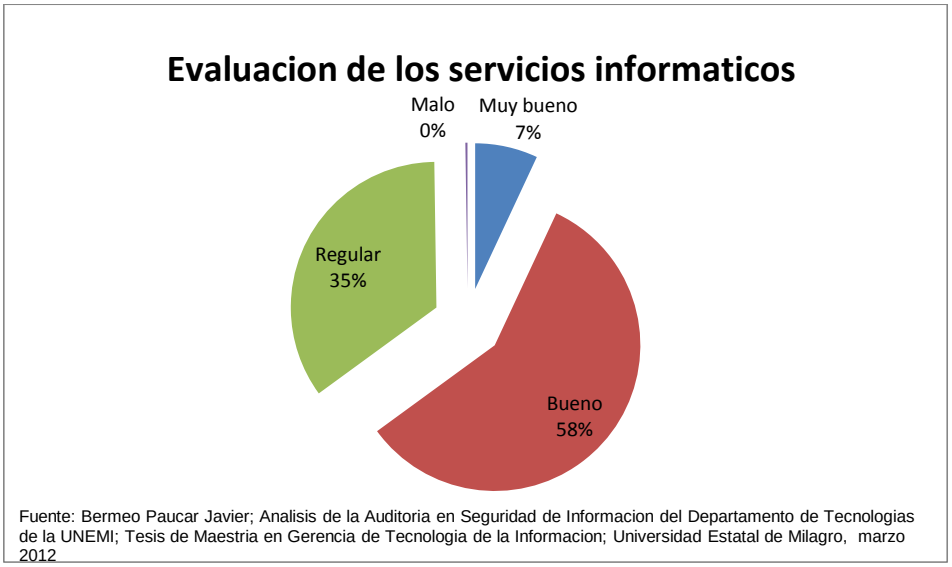
A pesar que 1 de cada 10, no específica la herramienta utilizada o no se encuentra en la lista propuesta ya que no la utiliza frecuentemente si no ocasionalmente para sus labores.

Conclusión.

Se puede indicar que para las labores de trabajo es más utilizado el paquete de office en un total del 70% lo cual la información almacenada en los equipos de cómputos es de gran importancia, igual de los que se guardan o almacenan en los servidores de datos que están en el departamento del TIC's por medio de los sistemas informáticos de la UNEMI

Pregunta 3

¿Cómo considera usted los servicios informáticos que presta el departamento del TIC's (sistemas, internet, correo, pagina web)?



Fuente: Bermeo Paucar Javier; Analisis de la Auditoria en Seguridad de Informacion del Departamento de Tecnologias de la UNEMI; Tesis de Maestria en Gerencia de Tecnologia de la Informacion; Universidad Estatal de Milagro, marzo 2012

Gráfico 6: Nivel de importancia de los servicios informáticos del TIC's.

Análisis.

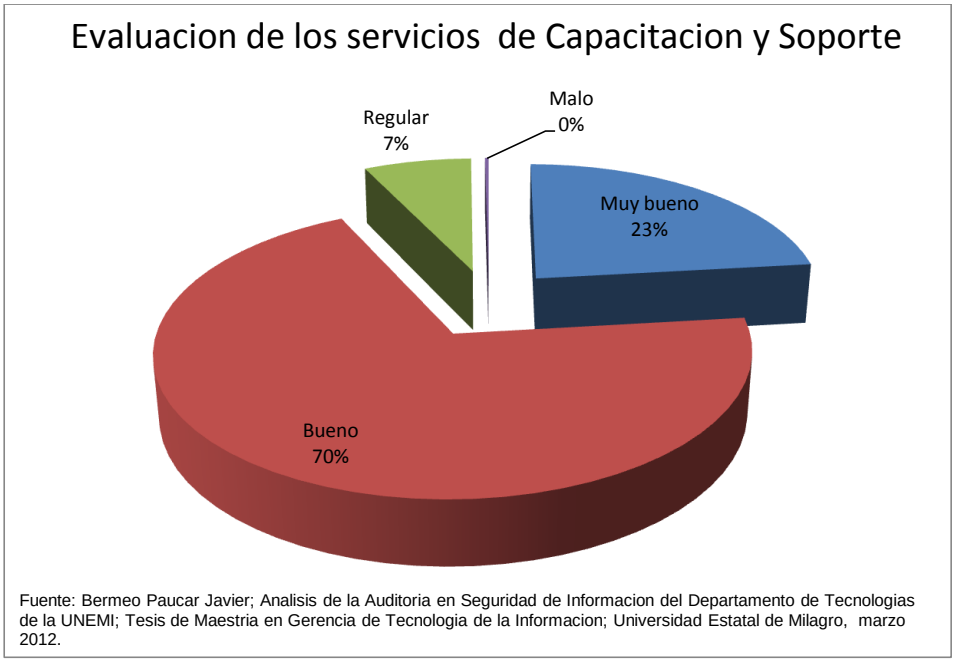
De acuerdo a la opinión de los empleados de la UNEMI se puede observar que hay una aceptación considerable 58% de los servicios que presta el departamento del TIC's y un 7% indica satisfacción total, pero también hay un porcentaje del 35% que no está satisfecha por los servicios que presta por lo que se debería considerar este porcentaje para verificar en que se está fallando.

Conclusión.

Se puede indicar que por el momento hay una satisfacción mayoritaria de los empleados de la UNEMI un 65% que indica que los servicios son buenos y un 35 % no está de acuerdo ya que indican que el servicio es malo o regular por lo que se debe poner atención a este porcentaje para mejorar el servicio y verificar que se está haciendo mal y corregir de manera que se pueda aumentar en mayor porcentaje la satisfacción de los usuarios.

Pregunta 4

¿Las capacitaciones y soportes técnicos recibidos de parte del Dpto. del TIC's como usted lo considera?



Fuente: Bermeo Paucar Javier; Analisis de la Auditoria en Seguridad de Informacion del Departamento de Tecnologias de la UNEMI; Tesis de Maestria en Gerencia de Tecnologia de la Informacion; Universidad Estatal de Milagro, marzo 2012.

Gráfico 7: Satisfacción Usuarios en capacitaciones y Soporte Técnico

Análisis.

El 70% de los usuarios entrevistados, indican que es bueno el servicio de capacitación y soporte técnico del TIC's y un 23% indican total aceptación por lo que deja ver al Departamento del TIC's que está preparado para ayudar en los inconvenientes que tiene el usuario con los equipos de computo, pero un 7% manifiesta que está en total desacuerdo por lo que indican que el soporte técnico y capacitación que brinda el TIC's no lo hacen de manera inmediata por lo que les retrasa con sus actividades.

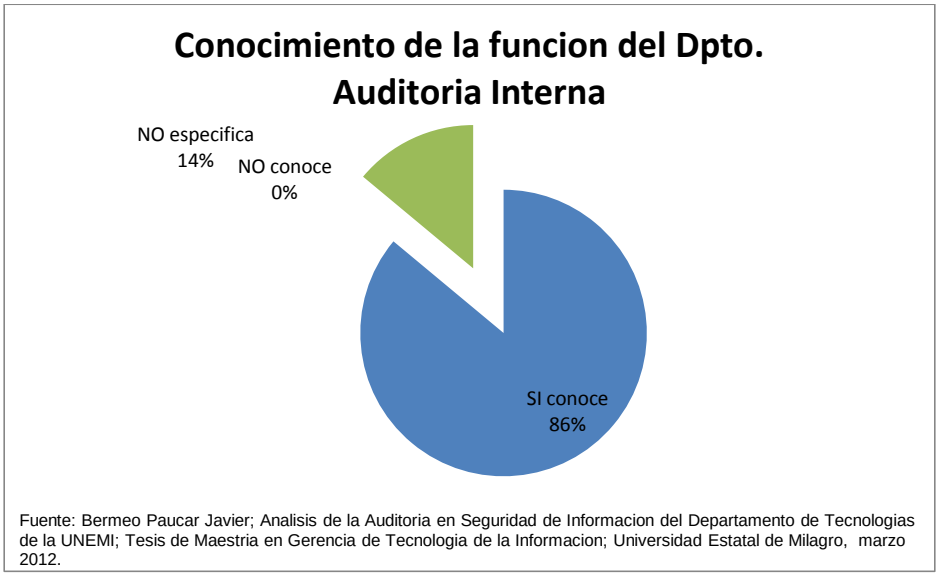
Conclusión.

El impacto positivo que se tiene en mayor porcentaje 93% indica que la labor que viene realizando el departamento del TIC's en capacitación y soporte a usuario es buena ya que solo un porcentaje mínimo no está de acuerdo por la demora que a veces tienen para brindarles el servicio que ellos solicitan.

Esto conlleva a que deben seguir mejorando para que nunca decayera el buen servicio que brindan a los usuarios.

Pregunta 5

¿Conoce usted cuál es su función del departamento de Auditoría Interna de la UNEMI?



Fuente: Bermeo Paucar Javier; Analisis de la Auditoria en Seguridad de Informacion del Departamento de Tecnologias de la UNEMI; Tesis de Maestria en Gerencia de Tecnologia de la Informacion; Universidad Estatal de Milagro, marzo 2012.

Gráfico 8: Conocimiento de la existencia del Dpto. Auditoría Interna

Análisis.

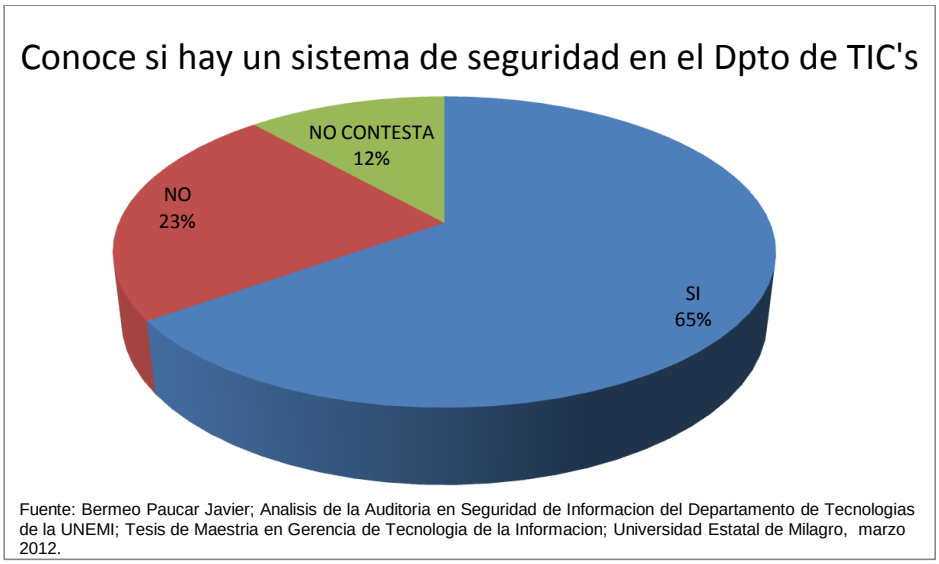
9 de cada 10 personas entrevistadas indican que si conocen la existencia del departamento de Auditoría Interna y de cuál es su función dentro de la universidad, de regular y controlar con los procedimientos que se realizan de acuerdo con las normas, políticas, reglamento y leyes que rige la Contraloría General del Estado y la Constitución del Ecuador. Pero un porcentaje mínimo 14% que representa a los que no contestaron, porque saben de la existencia del departamento de Auditoría Interna pero no saben a que se dedican con exactitud.

Conclusión.

Con el conocimiento que tiene los empleados de la existencia del Departamento de Auditoría Interna y de cuál es su función dentro de la universidad, se tiene un gran apoyo al realizar este proyecto que es de auditar al departamento del TIC's para observar sus falencias y poder corregir para que brinde un buen servicio tecnológico y de control.

Pregunta 6

Conoce usted si en el Departamento de Tecnología tiene algún sistema seguridad para ingresar a sus instalaciones?



Fuente: Bermeo Paucar Javier; Analisis de la Auditoria en Seguridad de Informacion del Departamento de Tecnologias de la UNEMI; Tesis de Maestria en Gerencia de Tecnologia de la Informacion; Universidad Estatal de Milagro, marzo 2012.

Gráfico 9: Conoce de sistema seguridad en el Dpto. TIC's.

Análisis.

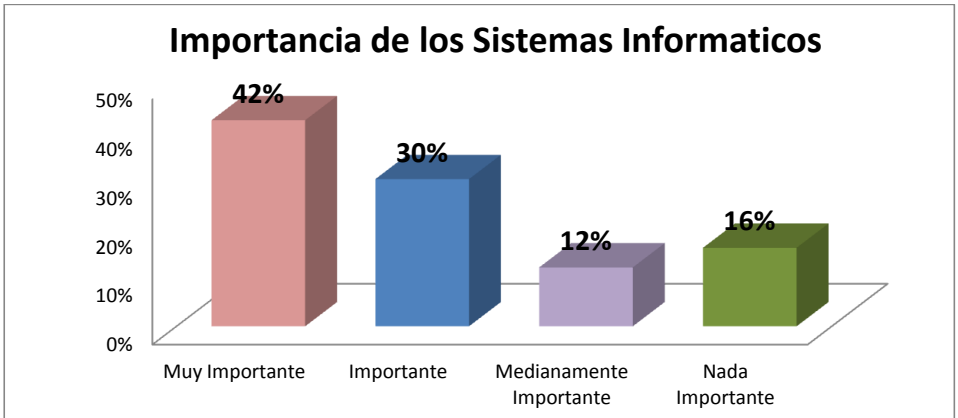
El personal encuestado en un 65% manifiesta que si existe un sistema de seguridad en el departamento de Tecnologías, ya que las veces que ha ido al departamento han tenido que recurrir a llamar para que abran la puerta de acceso para luego ser asignado algún personal que atienda sus inquietudes; pero un 23% de los encuestados manifiestan lo contrario que no existe seguridad por que han ido acompañados de alguien del TIC's o pasantes y han ingresado directamente sin ser llamados o direccionados al área que se requiere y más aun cuando no hay energía la puerta de acceso está inactiva y se ingresa con facilidad; y un 12% de las personas encuestadas manifiestan que no han ido al TIC's y no saben si hay o no algún sistema de seguridad para el ingreso al mismo. .

Conclusión.

Se debe tener en cuenta que para el departamento del TIC's, el control de acceso es primordial, tanto por el equipamiento que hay en él, como es la información almacenada en sus servidores, por lo tanto se debe temar en cuenta que hay personas que manifiestan poder acceder a él sin ningún control, por lo que es alarmante y preocupante y se debe tomar correctivos inmediatos sobre este punto.

Pregunta 7

Qué grado de importancia tiene los sistemas informáticos desarrollados por la UNEMI como herramienta de trabajo?



Fuente: Bermeo Paucar Javier; Analisis de la Auditoria en Seguridad de Informacion del Departamento de Tecnologias de la UNEMI; Tesis de Maestria en Gerencia de Tecnologia de la Informacion; Universidad Estatal de Milagro, marzo 2012.

Gráfico 10: Importancia sistemas Informáticos como herramienta de trabajo.

Análisis.

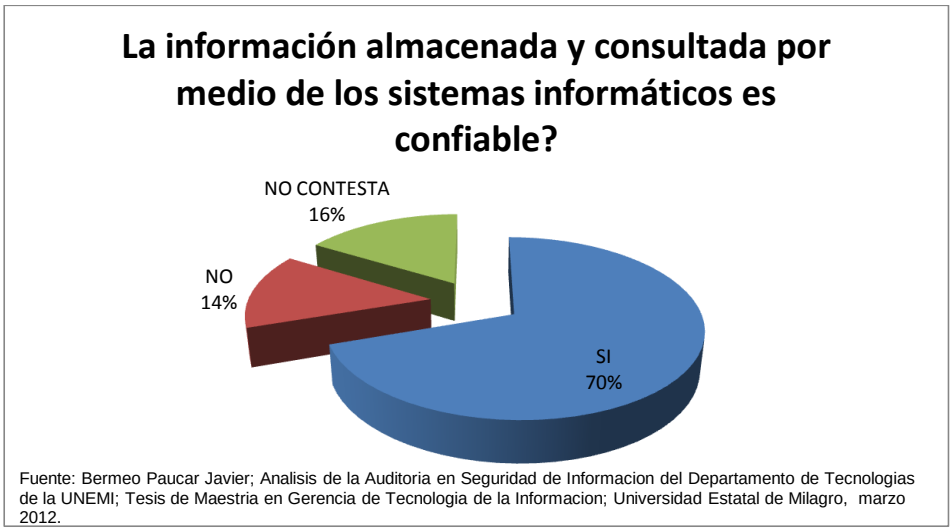
El 72% del personal encuestado indica que los sistemas Informáticos Académicos y Administrativos desarrollados por el TIC's tienen mucha importancia como herramienta de trabajo para ellos porque en la mayoría es en atención al público y deben interactuar con las herramientas mencionadas; en cambio hay un porcentaje mínimo del 12% que manifiesta que es medianamente importante por que realiza actividades o trabajos con los sistemas ocasionalmente, y un 16% de los encuestados manifiesta que no tiene mucha importancia los sistemas informáticos-UNEMI ya que no interactúan con ellos como herramienta de trabajo.

Conclusión.

Se puede concluir indicando que es de gran importancia para la mayoría de los empleados de la UNEMI que los sistemas informáticos desarrollados por el TIC's estén siempre activos o disponibles ya que es la principal herramienta de trabajo, y en un porcentaje mínimo lo utiliza ocasionalmente, por lo siempre hay que estar vigilando este servicio para atender de una manera eficiente.

Pregunta 8

¿La información almacenada y consultada por medio de los sistemas informáticos es confiable para usted?



Fuente: Bermeo Paucar Javier; Analisis de la Auditoria en Seguridad de Informacion del Departamento de Tecnologias de la UNEMI; Tesis de Maestria en Gerencia de Tecnologia de la Informacion; Universidad Estatal de Milagro, marzo 2012.

Gráfico 11: Información confiable de los sistemas informáticos

Análisis.

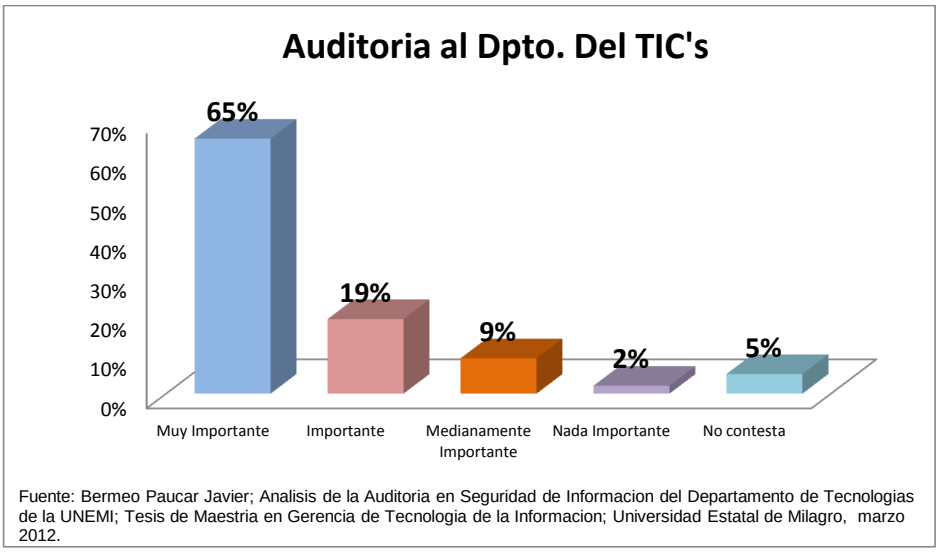
El 70% del personal encuestado, considera que si es confiable los datos que muestra los sistemas informáticos desarrollados por el TIC's, pero un 14% lo considera nada confiable por que según debe comparar con archivo e indica que la información es distinta a lo que almaceno o guardo por medio del sistema informático;, y un 16% no contesta por que manifiesta que no utiliza el sistema informático.

Conclusión.

Es importante el tener información confiable en el momento que se la necesite de manera rápida y oportuna que permita realizar nuestro trabajo de una manera eficiente, por lo que hay que tomar en cuenta lo manifestado por las personas que indican que el sistema falla en la presentación de su información en un porcentaje mínimo del 14%, que hay que mejorar para el futuro y tener un porcentaje del 0% de error.

Pregunta 9

¿Qué grado de importancia daría usted, si le consultan que se va auditar al departamento del TIC's?



Fuente: Bermeo Paucar Javier; Analisis de la Auditoria en Seguridad de Informacion del Departamento de Tecnologias de la UNEMI; Tesis de Maestria en Gerencia de Tecnologia de la Informacion; Universidad Estatal de Milagro, marzo 2012.

Gráfico 12: Importancia a la auditoria al departamento del TIC's.

Análisis.

El 84% de los encuestados manifiestan que están de acuerdo que se audite al departamento de Tecnologías (TIC's) ya que se quiere saber si están llevando adecuadamente los recursos informáticos y saber que políticas y procedimientos llevan para salvaguardar la información almacenada en los servidores y de los servicios que prestan; un 11% de los encuestados manifiesta que si auditan o no le da igual porque nunca ha tenido problemas con el sistema o servicios que presta el departamento del TIC's y un 5% no contesta por desconocimiento de lo que es auditar.

Conclusión.

La mayoría de los encuestados está de acuerdo de realizar una auditoría al departamento del TIC's por la importancia de los servicios que presta y de la información que se almacena en sus servidores y que políticas y procedimientos se están aplicando para precautelar la información y los equipos de computo.

La auditoria que se realiza dejara ver las falencias criticas que tiene el departamento de Tecnologías cuyo objetivo principal es mejorar y brindar un mejor servicio a la comunidad universitaria.

4.3 Relación entre objetivos e hipótesis.

Tabla 10: Conclusiones de Objetivos e Hipótesis

	Objetivos	**Hipótesis**	**Relación**
General	Realizar de una Auditoría Informática en el Departamento de Tecnología de la Información y Comunicaciones de la UNEMI con el fin de revelar las vulnerabilidades existentes en lo relativo a controles de seguridad informática.	El no contar con una auditoria de seguridad informática confiable está influyendo en los procesos del departamento del TIC's de la Universidad.	• Monitoreo de actividades • No importancia a seguridad informática
Particulares	Analizar cómo influye el no contar con una auditoria de seguridad informática sobre Políticas y Procedimientos que debe aplicarse en el Departamento del TIC'S de la UNEMI.	El no manejo adecuado de la información, la pérdida de información y la poca importancia que se da a la seguridad de in formación está influenciado por no contar con una auditoria de seguridad informática en el TIC's.	• Inventario de Equipos • Confiabilidad de la Información.

	Delimitar como está afectando negativamente no contar con una auditoria de seguridad informática en el Departamento del TIC'S de la UNEMI.	El acceso a lugares restringidos, mala utilización de software, y no aplicación de respaldos de información está influenciado por no contar con una auditoria de Seguridad Informática en el departamento del TIC's de la UNEMI.	• Comunicación entre oficinas • Poca agilización • Monitoreo
	Establecer una propuesta Tecnológica de una auditoria de seguridad informática para mejorar el desempeño laboral de los departamentos de la Universidad Estatal de Milagro.	El retraso de trabajo, en ocasiones es causado por no contar con políticas de Seguridad Informática sobre desastres informáticos en el departamento del TIC's de la Universidad Estatal de Milagro.	• Evaluación del Desempeño • Medición de Actividades • Monitoreo
	Establecer una estrategia para proponer en el Departamento del TIC'S de la UNEMI, una auditoria de seguridad informática.	El desarrollo de una planeación estratégica de realizar una auditoría en el departamento del TIC's sobre seguridad informática.	• Estrategia • Planificación

4.4 Verificación de las hipótesis.

La propuesta se desarrollará en base al análisis de resultados obtenidos de las entrevistas a los empleados que laboran en la Universidad Estatal de Milagro.

- ✓ El no contar con una auditoria de seguridad informática confiable está influyendo en los procesos del departamento del TIC's de la Universidad, ya que el desarrollo de una auditoria de seguridad informática en el departamento de Tecnología de la Información y Comunicaciones es aceptado por los empleados encuestados en un 93% ya que es de mucha importancia saber cómo se está llevando la seguridad informática con respecto a que políticas y procedimientos está empleando para brindar confiabilidad a todos quienes tienen relación directa con los sistemas informáticos y demás servicios que prestan como: correo electrónico, internet, respaldo de información, pagina web, telefonía y control de acceso, entre otros.

- ✓ El no manejo adecuado de la información, la pérdida de información y la poca importancia que se da a la seguridad informática está influenciado por no contar con una auditoria de seguridad informática en el TIC's. de la Universidad Estatal de Milagro ya que en una mayoría de los encuestados 70% indicaron que si confían en los datos almacenados en los servidores del TIC's ya que el resto manifestaron no utilizar los sistemas informáticos y un 14% dicen que no confían, y es con estos usuarios que se deberían trabajar para verificar el inconveniente y corregir, para esto se propone una auditoria al TIC's para observar en que se está fallando y corregir.

- ✓ El nivel de aceptación de los servicios prestados por el departamento del TIC's de la UNEMI es de un 65% estos servicios aportan de

manera directa o indirecta en el desarrollo de las actividades académicas y administrativas que se realizan, por lo que mejorar el grado de aceptación de estos servicios, dando a conocer, involucra también mejorar la satisfacción de usuarios y clientes en cuanto a su formación académica, aportando así al cumplimiento de los objetivos institucionales.

CAPÍTULO V
PROPUESTA DE SOLUCIÓN

5.1 Titulo de la propuesta.

Propuesta de una Auditoria de la Seguridad Informática del Departamento de Tecnologías en la Universidad Estatal de Milagro.

5.2 Fundamentación de la propuesta.

Para el departamento del TIC's, la realización de una auditoria de su seguridad informática es conveniente, porque les permitirá evaluar y tomar decisiones sobre aspectos importantes que tiene que ver con la información que se guardan en los servidores y equipos de cómputos que hay en el departamento y que son herramientas muy importantes para los servicios que ofrecen a toda la universidad.

Los beneficios de aplicar una auditoria de seguridad informática en el departamento del TIC's bien elaborado son inmediatos, ya que el departamento trabajará sobre datos e información levantada en la revisión de políticas, procedimientos y normas.

Además la Contraloría General del Estado, específica en las Normas de Control Interno para el Sector Público, en el Área de Sistemas de Información Computarizados lo siguiente:

5.2.1 Titulo: Sistemas de Información y Comunicación

Está constituido por los métodos establecidos para registrar, procesar, resumir e informar sobre las operaciones administrativas y financieras de una entidad. La calidad y oportunidad de la información que brinda el sistema afecta la capacidad de la máxima autoridad para adoptar decisiones adecuadas que permitan controlar las actividades de la entidad y preparar información confiable.

En el sector público el sistema integrado de información financiera se sustentará en una base de datos central y única, cuyo soporte será la informática y las comunicaciones, accesible para todos los usuarios de las áreas de presupuesto, tesorería contabilidad y deuda pública.

Los factores que conforman el sistema de información y comunicación son:

- Estrategias y sistemas integrados de información
- La calidad y oportunidad de la información
- Comunicación e información interna
- Comunicación e información externa
- Medios de comunicación
- Evaluación

5.2.2 ÁREA: Normas de Control Interno para el Área de Sistemas de Información Computarizados

5.2.2.1 TITULO: Organización del Área Informática

Cada entidad establecerá los lineamientos que orienten el proceso de organización del área de informática, aspecto que implica la definición de actividades a cumplir, las funciones y responsabilidades del personal, al igual que las interrelaciones de los elementos comprendidos en este sector con las áreas operativas de la entidad. Estos elementos formarán parte del Manual de Organización y Funciones, correspondientes.

La estructura básica del área de Informática estará constituida por áreas que son importantes para el funcionamiento, de acuerdo a las necesidades de cada entidad.

Corresponde a la máxima autoridad de la entidad aprobar las políticas que permitan organizar apropiadamente al área de informática y asignar los recursos humanos calificados y equipos de computación necesarios.

5.2.2.2 TITULO: Plan Informático, Adquisiciones o Actualización de Sistemas

Los sistemas de información computarizados se generan de acuerdo a los requerimientos o necesidades establecidas en cada entidad del sector público, y será necesario que la máxima autoridad apruebe un plan integral informático, con sujeción a las disposiciones vigentes. Dicho plan será de carácter obligatorio, independiente del nivel de complejidad o tamaño de la entidad, además será el que regule y determine el desarrollo informático de la institución a corto y mediano plazo.

5.3 Justificación de la propuesta.

Para la realización de una auditoria de seguridad informática en el departamento del TIC's entre a ejecución se debe tener la aprobación de una comisión o de la máxima autoridad el Consejo Universitario; por lo que se cuenta con el apoyo de ellos y es factible realizar esta auditoría en el departamento del TIC's.

Desde el punto de vista de una auditoria de seguridad informática, se debe contar con un conjunto de disposiciones o cursos de acción para llevarse a cabo en caso de presentarse situaciones de riesgo, a saber:

- Obtener una especificación de las aplicaciones, los programas y archivos de datos.
- Medidas en caso de desastre como pérdida total de datos, abuso y los planes necesarios para cada caso.
- Prioridades en cuanto a acciones de seguridad de corto y largo plazo.
- Verificar el tipo de acceso que tiene las diferentes personas al departamento, cuidar que los programadores no cuenten con acceso a la sección de operación y viceversa.
- Que los operadores no sean los únicos en resolver los problemas que se presentan.

5.4 Objetivos de la propuesta.

5.4.1. Objetivos Generales.

Realizar de una Auditoría Informática en el Departamento de Tecnología de la Información y Comunicaciones de la UNEMI con el fin de revelar las vulnerabilidades existentes en lo relativo a controles de seguridad informática.

5.4.2. Objetivos Específicos.

- Analizar cómo influye el no contar con una auditoria de seguridad informática sobre Políticas y Procedimientos que debe aplicarse en el Departamento del TIC'S de la UNEMI.
- Delimitar como afecta el no contar con una auditoria de seguridad informática en el Departamento del TIC'S de la UNEMI.
- Establecer una propuesta Tecnológica de una auditoria de seguridad informática para mejorar el desempeño laboral de los departamentos de la Universidad Estatal de Milagro.
- Establecer una propuesta en el Departamento del TIC'S de la UNEMI, de una auditoria de seguridad informática.

El cumplimiento de estos objetivos, busca ayudar ser más confiable y tener mayor grado de aceptación en los servicios que presta el departamento del TIC's, además de incidir en la disminución de los costos operativos y mejorar su organización administrativa al integrar políticas y procedimientos de seguridad informática que permitan salvaguardar la información y los equipos informáticos, para de esta manera mejorar su imagen departamental y de servicios

5.5 Ubicación sectorial y física.

El campo de aplicación de una auditoria informática es en el departamento del TIC's de la UNEMI, que se encuentra ubicado en el Ecuador, provincia del Guayas, Cantón Milagro, ciudadela Universitaria, edificio Bloque "R"; ya que con ello se podría evaluar y verificar cada una de las áreas que conforman del departamento.

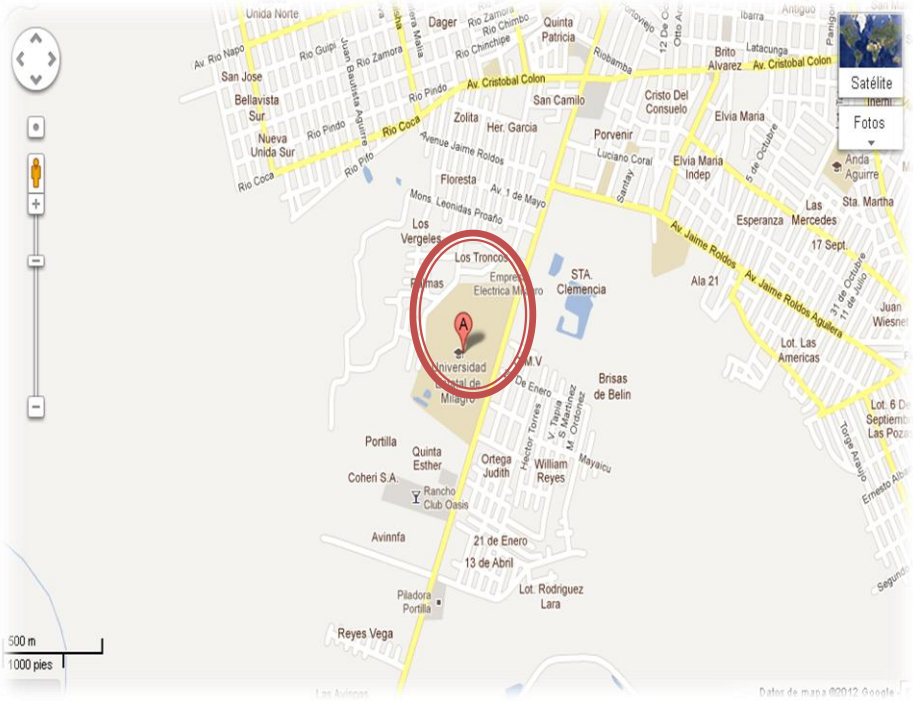


Gráfico 13: Ubicación de la Universidad Estatal de Milagro (Ubicación geográfica).

5.6 Factibilidad.

La puesta en marcha de la presente propuesta se define esencialmente en términos de la disponibilidad del recurso humano, esto es con el compromiso de participación conjunta de los empleados universitarios, los recursos económicos, recursos físicos (equipos e infraestructura), y materiales de oficina.

Por lo que la aplicación de una auditoria informática en el departamento del TIC's es beneficioso para el departamento y la Institución ya que se refleja en los siguientes puntos:

- Aumento de la productividad del personal del TIC's.
- Motivación del personal.
- Compromiso con la misión de la Universidad.
- Mejorar las relaciones laborales del departamento.
- Ayuda a formar equipos competentes,
- Mejorar la imagen departamental dentro de la Institución.

Por este motivo los mayores beneficiados con este proyecto serian todas las unidades académicas y departamentales de la Universidad Estatal de Milagro.

Sin embargo, como cualquier auditoria, se debe tener presente que son un instrumento muy potente y flexible, para la gestión del departamento. Por lo tanto, es evidente que las nuevas políticas y procedimientos que se implementen a futuro, son un elemento imprescindible y en continuo desarrollo dentro del TIC's.

Con estos antecedentes, y en función a la investigación realizada, se puede decir que 7 de cada 10 personas encuestadas quieren que se aplique una auditoria informática para verificar y comprobar que políticas y procedimientos se aplican para salvaguardar la información y equipos tecnológicos que se utiliza para la administración de los servicios que ofrece el departamento de Tecnología.

Se puede indicar que la propuesta de un análisis de la auditoria de información en el departamento del TIC's es factible, por el apoyo de los directivos y del personal UNEMI que va estar involucrado con este proyecto, equipamiento de una oficina y la disponibilidad de trabajar con equipos informáticos propios de la universidad.

.

5.7 Descripción de la propuesta.

“Propuesta para el desarrollo de una Auditoria de Seguridad Informática en el Departamento de Tecnología de la Información y Comunicaciones (TIC’s) de la Universidad Estatal de Milagro”

Las decisiones de realizar una auditoria informática dentro de cualquier departamento o institución, sin hacer diferencia de la actividad a la que se dedique, impacta en el proceso de actividades en que se viene laborando, es por ello que en el presente documento se plantean sugerencias para poder desarrollar una auditoria de seguridad de la información que este alineado a los objetivos de la institución y por ende se constituya un soporte en el desarrollo tecnológico y académico de la UNEMI favoreciendo el logro de los objetivos institucionales.

La auditoria que se plantea es para determinar cuál es el perfil adecuado en la implementación de las mejores prácticas, para llevar a cabo el desarrollo de prestar un mejor servicio con respecto a sistemas de información, telefonía, correo electrónico, pagina web , soporte usuario y capacitaciones, que permita llegar al cumplimiento de los objetivos del departamento del TIC’s y al mismo tiempo aportar a los objetivos institucionales favoreciendo también el proceso de acreditación de la UNEMI.

El aplicar una auditoria de seguridad informática nos dará pautas de lineamientos y políticas a seguir para estar protegidos de cualquier intento de robo o hurto de información y equipos informáticos que permitirán evaluar y conocer el aporte de los servicios que brinda y administra el TIC’s para con el cumplimiento de los objetos institucionales.

La auditoria de la seguridad informática se debería desarrollar en el departamento de Auditoria Interna o en una oficina provisional que acondicione con acceso a los equipos informáticos (PC, servidores, telefonía) del TIC’s, software de utilitarios, sistemas informáticos (desarrollados en la UNEMI), conexión a internet sin restricción y la información por parte del personal del departamento del TIC’s y

departamentos que utilicen sus servicios informáticos y tecnológicos para el levantamiento de información, información que se evaluara bajo las siguientes normativas:

5.7.1 NORMATIVAS EMPLEADAS

Para la realización de la presente Auditoría de Seguridad Informática se utilizaron los siguientes estándares y guías:

1. ESTÁNDARES:

- COBIT (Control Objectives for Information Technology)
  - "Audit Guide lines" 3ra. Edición. COBIT, fechado en Julio de 2008.
  - "Control Objectives" 3ra. Edición. COBIT, fechado en Julio de 2008.
- ISO (International Standard Organization)
  - "Estándar de Seguridad ISO 17799" (British Standard 7799)
- DoD (Department of Defense of the United States) Rainbow Series Library
  - "Trusted Network Interpretation of the TCSEC" (TNI), 31 July 1987. (Red Book), National Computer Security Center (NCSC).
  - "Password Management Guideline", 1990. (Green Book)
- Contraloría General del Estado - Normas de Control Interno.
- Legislación del Ecuador – Infracciones sobre delitos informáticos.

Legislación - Ecuador

Gráfico 14: Normativa Legislación del Ecuador

Infracciones Informáticas (CPP)

INFRACCIONES INFORMATICAS	REPRESION	MULTAS
Delitos contra la información protegida (CPP Art. 202)		
1. Violentando claves o sistemas	6 m. - 1 año	$500 a $1000
2. Seg. nacional o secretos comerciales o industriales	3 años	$1.000 - $1500
3. Divulgación o utilización fraudulenta	3 a 6 años	$2.000 - $10.000
4. Divulgación o utilización fraudulenta por custodios	9 años	$2.000 - $10.000
5. Obtención y uso no autorizados	2 m. - 2 años	$1.000 - $2.000
Destrucción maliciosa de documentos (CCP Art. 262)	6 años	---
Falsificación electrónica (CPP Art. 353)	6 años	---
Daños informáticos (CPP Art. 415)		
1. Daño dolosamente	6 m. - 3 años	$60 – $150
2. Serv. público o vinculado con la defensa nacional	5 años	$200 - $600
3. No delito mayor	8 m. - 4 años	$200 - $600
Apropiación ilícita (CPP Art. 553)		
1. Uso fraudulento	6 m. - 5 años	$500 - $1000
2. Uso de medios (claves, tarjetas magnéticas, etc.)	5 años	$1.000 - $2.000
Estafa (CPP Art. 563)	5 años	$500 - 1.000

Gráfico 15: Infracciones Informáticas

2. GUÍAS DE REFERENCIA Y SOPORTE:

- ISACA (Information Systems Audit and Control Association)
  - "Planning the IS Audit" ISACA, 1998.
  - "Normas generales para la auditoría de los sistemas de
  - Información" ISACA, 1997.
- NIST (National Institute of Standards and Technology - U.S. Department of Commerce)
  - "Generally Accepted Principles and Practices for Securing Information Technology Systems". Marianne Swanson y Barbara Guttman, 1996.
  - "Guide for Developing Security Plans for Information Technology Systems" Marianne Swanson, 1998.
  - "Security Self-Assessment Guide for Information Technology Systems" Marianne Swanson, 2001.
  - "Automated Tools for Testing Computer System Vulnerability" W. Timothy Polk, 1992.
  - "The Common Criteria for Information Technology Security Evaluation" v2.1 (ISO IS 15408)
- Cisco Systems
  - "Cisco SAFE: A Security Blueprint for Enterprise Networks". Sean Convery y Bernie Trudel, Cisco Systems. 2000.
  - "Beginner's guide to network security" Cisco Systems. 2001
- "Tutorial de seguridad" CERT (Computer Emergency Response Team).
- "Handbook of Information Security Management" Hal Tipton and Micki Krause, Consulting Editors, 1998.
- "Internet Security Professional Reference, Second Edition" Autores multiples, New Riders Publishing, 1997.

5.8 Análisis financiero.

5.8.1 Inversión Presupuestada del Plan General

Tabla 11: Inversión Presupuestada horas extras

Inversión	Valor	Núm. de meses	Total
Auditor de S.I.	$300,00	6	$ 1800,00
Encuestadores	$ 100,00	1	$ 100,00
Ayudante	$ 200,00	6	$ 1200,00
Enlace Internet	$ 90,00	6	$540,00
Servicios básicos	$ 180,00	6	$ 1080,00
		Total	$ 4.720,00

5.8.2 Ingresos

El departamento del TIC's depende del presupuesto anual asignado a la Universidad Estatal de Milagro que es una institución educativa gubernamental, por ende sus ingresos son asignados de forma anual en base a un presupuesto Institucional y remitido al el Ministerio de Finanzas quien que es el encargado de revisar y analizar dicho presupuesto para su aprobación o emitir las observaciones de acuerdo a su criterio.

Al ejecutar el proyecto planteado de una Auditoria de Seguridad Informática por desarrollado por estudiantes de posgrado avalado por el departamento de Auditoría Interna de la Institución, la universidad obtendría un ahorro por concepto de:

- Asesoramiento externo de una Autor.
- Reducir costo en materiales de oficina y suministros
- Reducir costos por alquiler de equipos

Asesoramiento externo

Valor	Numero empleados	Meses	Total mes
$ 1000,00	1	6	$ 6.000,00
$ 1000,00	1	1	$ 1.000,00

Tabla 12: Gasto Asesoramiento Externo

Materiales y Suministros

	Costo unitario	# Mat. Y Sum.	Valor Total	Copias por tóner
Resma hojas tamaño A4	$ 7,00	2	$ 14,00	1000
Tóner	$ 350,00	1	$ 350,00	5000

Tabla 13: Materiales y Suministros

PC/Servidor

Equipos	Costo	Total mes	Valor Total
1	$ 750	6	$ 750,00

Tabla 14: Gasto Pc/servidor.

5.8.3 Gastos y Costos

La Universidad Estatal de Milagro cuenta con la infraestructura necesaria para la realización de la presente propuesta, equipos de computo, internet, telefonía, Dpto. de Auditoría Interna, oficinas y material de oficina, así como con el talento humano para ejecutar y puesta en marcha de la auditoria de la Seguridad Informática del Dpto. del TIC's, por lo que la universidad no incurrirá en mayores gastos.

La propuesta de una auditoría se puede presentar como parte de los proyectos anuales del departamento de Auditoría Interna por lo que sería considerado dentro de las actividades de personal que laboran en dicho departamento los mismos que tienen ya establecido un sueldo incluido dentro del presupuesto anual de la universidad, al ser la auditoria un proyecto que está dentro de las responsabilidades del personal que se asigne para su desarrollo y posterior ejecución, se considera un pago aproximado al personal por su participación en el proyecto y posterior ejecución y seguimiento, gastos que se detallan en las siguientes tablas:

Servicios básicos (Luz, Agua, Teléfono, Oficina, Video proyector, climatización, Audio) e internet

	Costo total	**Total meses**	**Costo total**
Servicios básicos	180	6	$ 1080
Internet	90	6	$ 540

Tabla 15: Gasto Servicios básicos

Desarrollo y ejecución del Proyecto

	Costo mes	Uso por mes	Total
Costo por encuesta	$ 100	1	$ 100,00
Asistente	$ 200	6	$ 1200,00
Auditor S.I.	$ 300	6	$ 1800,00
Total mes	$ 600		$ 3.100,00

Tabla 16: Gasto Empleados horas extras

	Ingresos	Egresos	Crecimiento
Periodo 1	$ 8114,00	$ 4720,00	-----
Periodo 2	$ 8519.70	$ 4956.00	5%
Periodo 3	$ 9116.08	$ 5302.92	7%

Tabla 17: Ingresos y Egresos

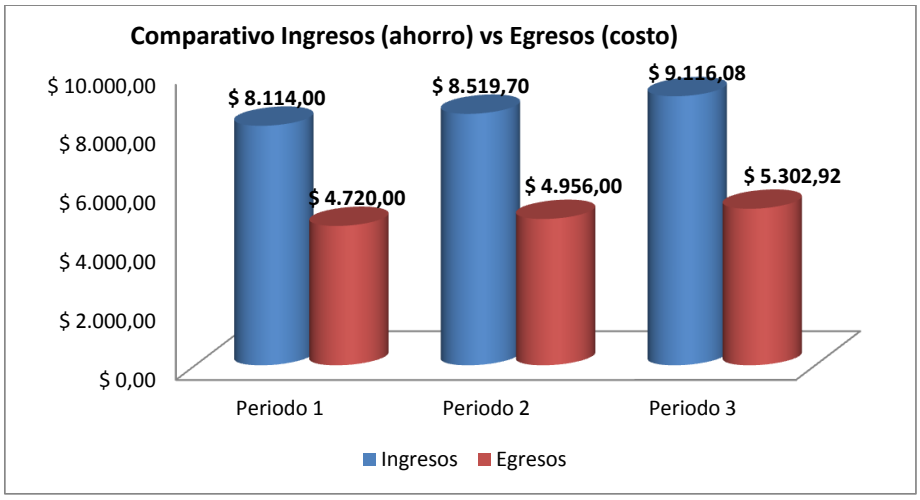


Grafico 16: Comparativo de Ingresos y Egresos

~~Utilidad Bruta~~ cada 6 meses

Periodo ~~1~~	$ 3.394,00
Periodo ~~2~~	$ 3563,70
Periodo ~~3~~	$ 3.813,16

Tabla 18: Utilidad Bruta

5.8.4

Análisis de Factibilidad por Evaluación Financiera

Con formato: Normal, Sin viñetas ni numeración

Para realizar una Auditoria de Seguridad Informática en el departamento del TIC's, se tiene como objetivo mejorar el desarrollo de los procedimientos y políticas de seguridad para brindar un mejor servicio y confiabilidad en los datos almacenados en los servidores (data center), y dar a conocer a la comunidad universitaria los diferentes servicios que ofrece el TIC's y como acceder a ellos, además ayudar a cumplir con los objetivos del departamento del TIC's, así también como de toda la UNEMI, por lo tanto el apoyo de los directivos es vital, y este apoyo existe para todo el proyecto, ya que se

constituye en un eje importante que contribuya a mejorar los servicios informáticos con miras de apoyo, para la obtención de la acreditación universitaria.

Con la ejecución de la presente propuesta se pueden mencionar ciertos beneficios para el Departamento del TIC's como para la universidad:

- Aporte al proceso de la acreditación Universitaria, la administración y uso de los recursos de tecnológicos van a constituir con un indicador importante al momento de la acreditación, ya que existirá una percepción positiva por parte de los usuarios y clientes quienes son los beneficiados directamente con la mejora de la seguridad de información y equipos tecnológicos.

- Satisfacer eficientemente en el uso de los recursos de Tecnológicos en las jornadas académicas, lo que permitiría un mayor desarrollo y preparación de los estudiantes, aportando así a que un mayor número de estudiantes se beneficien de los servicios informáticos y que su preparación académica sea coherente a la demanda del mercado laboral.
- Motivación del personal del TIC's.
- Compromiso con la misión de la Universidad.
- Mejorar las relaciones laborales del departamento.
- Ayuda a formar equipos competentes,
- Mejorar la imagen departamental dentro y fuera de la Institución.

Por este motivo los mayores beneficiados de este proyecto serian las unidades académicas y departamentos de la Universidad Estatal de Milagro, cuyo objetivo periódico es de realizar auditorías en el departamento del TIC's para evaluar las mejoras que se realizan en el departamento de brindar un mejor servicio.

5.8.5 VAN, TIR y Periodo de Recuperación

Valor Actual Neto

En VAN mide la productividad de un proyecto de forma absoluta, calculando la cantidad total que ha aumentado el capital como consecuencia del desarrollo del proyecto.

La regla de aceptación de un proyecto para el VAN es: VAN >= 0.

Si tomamos en cuenta la tasa de crecimiento del 8,3% obtendremos un ingreso de $5.111,76 en nuestra propuesta, considerando la regla de aceptación podemos decir que la propuesta es realizable.

Tasa Interna de Retorno o Tasa de Inversión de Retorno

Se obtiene para la presente propuesta un TIR del 43%, ya que nuestra propuesta de desarrollo de la Auditoria de Seguridad Informática en una inversión, se concluye que la rentabilidad de la propuesta es aceptable. El TIR expresa el crecimiento del capital de la propuesta y la tasa de crecimiento del capital por 3 periodos.

Periodo de Recuperación

Inversión	($ 4720,00)	($ 4720,00)
Periodo 1	$ 3.394,00	$ (1.326,00)
Periodo 2	$ 3.563,70	$ 2.237,70
Periodo 3	$ 3.813,16	$ 6.050,86

Tabla 19: Periodo de Recuperación.

Tiempo de recuperación en meses	
1,59	9,5 meses

Al realizar o invertir en un proyecto, lo que se espera es obtener un beneficio o utilidades, para la propuesta de realizar una Auditoria de Seguridad Informática en el departamento del TIC's, la inversión del capital se recupera en el segundo periodo, es decir que en el segundo periodo el flujo de caja igualara la inversión inicial, luego del cual ya se puede observar la rentabilidad de la propuesta.

5.8.6 Flujo de Caja

Tabla 20: Flujo de Caja.

	Enero	Febrero	Marzo	Abril	Mayo	Junio
Egresos						
Servicios básicos	$ 180,00	$ 180,00	$ 180,00	$ 180,00	$ 180,00	$ 180,00
Sueldos Horas extras						
Auditor SI	$ 300,00	$ 300,00	$ 300,00	$ 300,00	$ 300,00	$ 300,00
Encuestas (Pasantes)	$ 100,00	$ 0,00	$ 0,00	$ 0,00	$ 0,00	$ 0,00
Asistente	$ 200,00	$ 200,00	$ 200,00	$ 200,00	$ 200,00	$ 200,00
Enlace Internet	$ 90,00	$ 90,00	$ 90,00	$ 90,00	$ 90,00	$ 90,00
Total Egresos	**$ 870,00**	**$ 770,00**	**$ 770,00**	**$ 770,00**	**$ 770,00**	**$ 770,00**
Ingresos (Ahorros)						
Papelería	$ 2,33	$ 2,33	$ 2,33	$ 2,33	$ 2,33	$ 2,33
Suministros impresora	$ 58,33	$ 58,33	$ 58,33	$ 58,33	$ 58,33	$ 58,33
Asesoramiento externo	$ 1.000,00	$ 1.000,00	$ 1.000,00	$ 1.000,00	$ 1.000,00	$ 1.000,00
Servidor/Pc	$ 750,00	$ 750,00	$ 750,00	$ 750,00	$ 750,00	$ 750,00
Total Ingresos	**$ 1.810,66**	**$ 1.810,66**	**$ 1.810,66**	**$ 1.810,66**	**$ 1.810,66**	**$ 1.810,66**
Utilidad Bruta	**$ 940,66**	**$ 1.040,66**	**$ 1.040,66**	**$ 1.040,66**	**$ 1.040,66**	**$ 1.040,66**

5.9 EJECUCIÓN Y OPERACIÓN

5.9.1 EJECUCIÓN

Para el desarrollo y ejecución de la propuesta de una Auditoria de Seguridad Informática en el departamento del TIC's se plantea un plan de desarrollo, el mismo que se detalla a continuación:

AUDITORÍA DE SEGURIDAD INFORMÁTICA

OBJETIVO GENERAL

Consiste en la realización de una Auditoría Informática al Departamento de Tecnología de la Información y Comunicaciones de la Universidad Estatal de Milagro (TIC's), con el fin de revelar las vulnerabilidades existentes en lo relativo a controles de seguridad, como medio para el desarrollo de una Política de Seguridad informática, donde se definirán los lineamientos para promover la implementación de un modelo de seguridad informática en toda la Universidad.

ALCANCE

La Auditoría de seguridad Informática propuesta comprende fundamentalmente la planificación y ejecución de los siguientes aspectos:

1. EVALUACIÓN DE LA SEGURIDAD LÓGICA

1.1. Identificación de usuarios
1.2. Autenticación de usuarios
1.3. Password
1.4. Segregación de funciones

2. EVALUACIÓN DE LA SEGURIDAD EN LAS COMUNICACIONES

2.1. Topología de red
2.2. Comunicaciones externas
2.3. Configuración lógica de red
2.4. Mail
2.5. Antivirus
2.6. Firewall
2.7. Ataques de red

3. EVALUACIÓN DE LA SEGURIDAD DE LAS APLICACIONES

3.1. Software

3.2. Seguridad de bases de datos

3.3. Control de aplicaciones en PC´s

3.4. Control de datos en las aplicaciones

3.5. Ciclo de vida del desarrollo del software

4. EVALUACIÓN DE LA SEGURIDAD FÍSICA

4.1. Equipamiento

4.2. Control de acceso físico al Dpto. Tecnologías

4.3. Control de acceso a equipos

4.4. Dispositivos de soporte

4.5. Estructura del edificio

4.6. Cableado estructurado

5. EVALUACIÓN DE LA ADMINISTRACIÓN DEL CPD (Data center)

5.1. Administración del CPD

5.2. Capacitación de usuarios

5.3. Backup

5.4. Documentación

6. EVALUACIÓN DE LAS AUDITORÍAS Y REVISIONES

6.1. Chequeos del sistema

6.2. Responsabilidad de los encargados de seguridad

6.3. Auditorias de control de acceso

6.4. Auditorías de redes

7. EVALUACIÓN DEL PLAN DE CONTINGENCIAS

7.1. Plan de administración de incidentes

7.2. Backup de equipamiento

7.3. Estrategias de recuperación de desastres

METODOLOGÍA APLICADA

La metodología utilizada para la realización de la presente Auditoría Informática se basa en el desarrollo de las siguientes actividades:

a. Definición de los objetivos de la auditoría y delimitación del alcance.
b. Análisis de fuentes de datos y recopilación de información.
c. Generación del plan de trabajo, asignación de recursos y establecimiento de plazos de tiempo.
d. Generación de cuestionarios y adaptaciones realizadas a los mismos en base a los perfiles de los entrevistados.
e. Proceso de recolección de información:
e.1 Entrevistas a:

- Responsable del Departamento de Tecnologías: Director TIC's.
- Personal del Departamento Tecnologías: Jefe Desarrollo, Programadores, Administrador Operaciones, Asistente de Operaciones, Administrador Base de Datos, Coordinador Infraestructura y Asistentes de Infraestructura.
- Usuarios de los sistemas: personal del área administrativa y académicos.
- Especialistas externos: especialista en LINUX y redes informáticas; Auditor de Sistemas, certificado por CISA.

e.2 Reconocimiento del entorno y del ámbito de trabajo.
f. Desarrollo de un análisis de riesgos.
g. Análisis de los datos recolectados, hallazgos de debilidades y generación de recomendaciones.

NORMATIVAS EMPLEADAS

Para la realización de la presente Auditoría de Seguridad Informática se utilizaron los siguientes estándares y guías:

1. ESTÁNDARES:

- COBIT (Control Objectives for Information Technology)
  - "Audit Guide lines" 3ra. Edición. COBIT, fechado en Julio de 2008.
  - "Control Objectives" 3ra. Edición. COBIT, fechado en Julio de 2008.

- ISO (International Standard Organization)
  - “Estándar de Seguridad ISO 17799” (British Standard 7799)
- DoD (Department of Defense of the United States) Rainbow Series Library
  - “Trusted Network Interpretation of the TCSEC” (TNI), 31 July 1987. (Red Book), National Computer Security Center (NCSC).
  - “Password Management Guideline”, 1990. (Green Book)
- Normas de Control Interno.

2. GUÍAS DE REFERENCIA Y SOPORTE:

- ISACA (Information Systems Audit and Control Association)
  - “Planning the IS Audit” ISACA, 1998.
  - “Normas generales para la auditoría de los sistemas de
  - Información” ISACA, 1997.
- NIST (National Institute of Standards and Technology - U.S. Department of Commerce)
  - “Generally Accepted Principles and Practices for Securing Information Technology Systems”. Marianne Swanson y Barbara Guttman, 1996.
  - “Guide for Developing Security Plans for Information Technology Systems” Marianne Swanson, 1998.
  - “Security Self-Assessment Guide for Information Technology Systems” Marianne Swanson, 2001.
  - “Automated Tools for Testing Computer System Vulnerability” W. Timothy Polk, 1992.
  - “The Common Criteria for Information Technology Security Evaluation” v2.1 (ISO IS 15408)
- Cisco Systems
  - “Cisco SAFE: A Security Blueprint for Enterprise Networks”. Sean Convery y Bernie Trudel, Cisco Systems. 2000.
  - “Beginner's guide to network security” Cisco Systems. 2001
- “Tutorial de seguridad” CERT (Computer Emergency Response Team).
- “IT Baseline Protection Manual - Standard security safeguards”. Bundesanzeiger – Verlag, Alemania. 2001.

- “Handbook of Information Security Management” Hal Tipton and Micki Krause, Consulting Editors, 1998.
- “**Internet Security Professional Reference**, Second Edition” Autores multiples, New Riders Publishing, 1997.

INFORME DE RECOLECCION DE INFORMACION

La organización a auditar, es la Universidad Estatal de Milagro, Dpto. de Tecnologías, es una Institución Educativa, con aproximadamente 325 empleados, distribuidos en las diferentes áreas; en el Dpto. de Tecnologías está compuesto por 4 áreas: Desarrollo, Base de Datos, Infraestructura y Administración Operaciones y el total del personal que labora ahí es de 13 empleados.

La estructura jerárquica del Dpto. de Tecnologías se muestra en el organigrama presente.

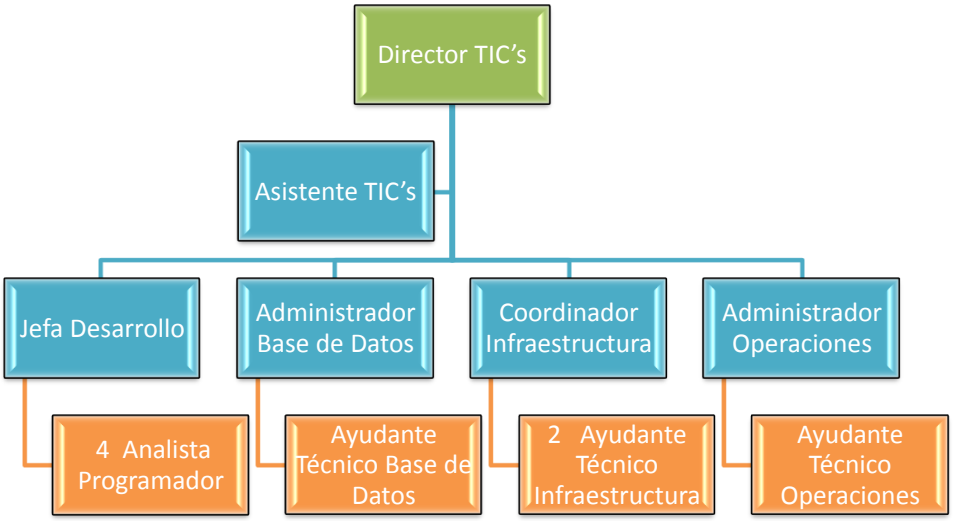


Grafico 17: Organigrama del Departamento del TIC's.

A continuación se describen los datos y la información recogida durante el levantamiento realizado en la UNEMI, detallando cada uno de los controles que se implementan en la actualidad.

1. EVALUACION DE LA SEGURIDAD LÓGICA

OBJETIVO DE AUDITORÍA: los auditores deberán evaluar los controles de accesos de los usuarios a las plataformas de procesamiento informático y a los datos que éstas gestionan, con el fin de señalar las irregularidades que obstaculicen la confidencialidad, exactitud y disponibilidad de la información, y las mejoras que fueran factibles de efectuarse.

1.1 IDENTIFICACIÓN DE USUARIOS

1.1.1 ALTAS

Cuando un usuario nuevo ingresa a la empresa, el área de Recursos Humanos toma sus datos, dando de alta su USER sin embargo, no existe un procedimiento formal a seguir para realizar estas tareas. Si este usuario necesita del sistema informático, Recursos Humanos hace el pedido al Departamento del ODI, donde se genera los permisos del usuario al sistema. Los datos que se ingresan en la cuenta son los siguientes:

- ID de usuario, inicialmente será compuesto por la inicial del primer nombre, seguido por su primer apellido y la inicial de su segundo apellido, esto inicialmente se lo hacía manualmente, pero en la actualidad se lo hace automáticamente desde que se registra sus datos en el sistema de Recursos Humanos.
- Password, inicialmente será el número de cedula, y se instruye al usuario para que lo modifique.
- Nombre y apellido completo, se obtiene del archivo de Recursos Humanos.
- Grupo al que pertenece, según el área de la Universidad que le fue asignada por el Departamento de Recursos Humanos. Pudimos comprobar que en algunos casos este campo permanece vacío permitiendo que el usuario

acceda a todos los menús del sistema o que no pueda ver opciones del sistema donde debe pertenecer a un grupo especifico

- Fecha de expiración del password indefinido el tiempo, permitiendo que nunca se actualice la contraseña.
- Fecha de anulación de la cuenta para dar de baja la cuenta.
- Contador de intentos fallidos, no se bloquea el login si el contador es igual a tres o más (si el usuario ha ingresado mal la contraseña tres veces seguidas).
- Autorización de imprimir ya que no todos los usuarios pueden imprimir los datos del sistema.
- Autorización de ingreso a la base de datos ya que no todos los usuarios tienen acceso a los datos de este sector.

1.1.2 BAJAS

Las cuentas de los usuarios no se eliminan del sistema, se deshabilitan manualmente actualizándoles la cuenta. De esta forma los datos de las cuentas dadas de baja quedan almacenados en el disco y no es posible repetir los ID´s de usuarios anteriores para nuevos empleados.

No hay ningún procedimiento formal para dar de baja un usuario del sistema. El departamento de Recursos Humanos informa al Dpto. del ODI, y allí se procede a dar de baja el empleado una vez que se ha desvinculado de la universidad.

1.1.3 MANTENIMIENTO

No se lleva a cabo ninguna revisión periódica ni control sobre el buen funcionamiento de las cuentas de los usuarios, ni sobre los permisos que tienen asignados.

1.1.4 PERMISOS

El control de acceso en la universidad no se basa en los perfiles de los usuarios y la asignación o denegación de permisos a los mismos, sino más bien en perfiles de grupos. Estos grupos se generan en concordancia con las áreas y es el Departamento de Recursos Humanos el que asigna cada usuario a un grupo determinado. Luego, los usuarios son dados de alta en el sistema, y los administradores del sistema son los encargados de la asignación de permisos.

El sistema informático está desglosado en una gran cantidad módulos diferentes, donde cada uno de ellos es un programa en sí mismo. De esta manera cada usuario del sistema, según el grupo al que pertenece en la universidad, dispone de los accesos directos a los programas que corresponden a su área. Así, los usuarios solo pueden interactuar con los datos a los que dichos módulos les permiten acceder. Los accesos directos a los que el usuario tiene acceso los genera el administrador de Operaciones a mano, una vez que el usuario fue dado de alta.

A medida que la responsabilidad del usuario en la universidad es mayor, son necesarios más datos, y por ende más módulos, o accesos a programas. Esto quiere decir que en un cargo de Jefe de área puede haber varios módulos disponibles, mientras que a modo de ejemplo, los asistentes solo tienen un módulo de consulta de datos. Comprobamos que en ciertos casos sobran funcionalidades. A modo de ejemplo, toda el área de Unidades Académicas (sistema matriculación) tiene disponible un mismo menú, aunque haya funciones que ciertos empleados no necesiten, y al tratar de acceder a datos críticos el sistema requerirá nuevamente el usuario y el password. Este control sirve para comprobar que el usuario logeado es el mismo que está intentando acceder a estos datos sensibles, de manera que si este segundo login no coincide con el primero, los datos no serán mostrados.

No existe en el sistema informático una lista de control de acceso que se utilice para identificar los tipos de permiso que tiene cada usuario con respecto a los datos. Solo existe una relación entre las áreas de la universidad, los menús y los usuarios correspondientes a cada área, y en las carpetas de documentación del desarrollo relativas a cada módulo de programa se explica la relación que existe entre cada módulo de programa y los datos. Al no existir esta lista de control de acceso, resulta complicado identificar qué datos se puede modificar cada usuario.
No se tiene en cuenta ninguna restricción horaria para el uso de los recursos. Tampoco se considera una restricción física sobre la máquina desde donde se conecta (logea) cada usuario.

1.1.5 INACTIVIDAD

Si el usuario permanece un período de tiempo conectado (logeado) sin actividad, el sistema no ejecuta ninguna acción; los administradores solo advierten a los usuarios sobre la necesidad de no dejar las máquinas conectadas (logeadas) e inactivas.

Si las cuentas de usuarios permanecen varios días sin actividad, por licencias o por vacaciones no pasan a un estado de suspensión.

1.1.6 CUENTAS DE USUARIO

Los usuarios de la universidad son identificados en forma personal, pero utilizan el mismo usuario y contraseña para ingresar a los sistemas informáticos, equipos informáticos y correo electrónico por medio del servidor LDAP.

Los usuarios del sistema pueden tener abiertos, al mismo tiempo, todos los menús a los que están autorizados, y varias sesiones del mismo menú. No se hacen restricciones en cuanto a la cantidad de sesiones que los usuarios pueden utilizar simultáneamente.

En la universidad hay tres o cuatro personas con perfil de administrador. Cada una de ellas tiene su cuenta con un password personal, pero a fines prácticos, ellos pueden resetear todas los password de las demás cuentas, ya que no hay una clara definición de tareas. Además, el administrador puede logearse desde cualquier terminal de la universidad lo que resulta riesgoso ya que podría, por error, abandonar ese puesto de trabajo dejando esa terminal logeada con su usuario administrador.

Existe, además, soporte de mantenimiento externo (pasantes) que utiliza la misma cuenta del administrador para hacer modificaciones en los sistemas operativos, ya que el administrador de operaciones del TIC's le suministró el password. Una vez finalizado el mantenimiento, el administrador del sistema no cambia la contraseña, de manera que ésta continúa siendo conocida por personal externo.

1.2 AUTENTICACIÓN

En la pantalla de conexión (login) de los sistemas se muestran los siguientes datos:

Nombre de usuario (a completar por el usuario),

Password (a completar por el usuario),

Cuando un usuario ingresa su password al sistema, aparecen asteriscos en lugar de mostrar el dato que está siendo ingresado. Una vez que algún usuario ha logrado logearse en el sistema, aparece en la parte de debajo de la pantalla el nombre del usuario logeado.

Dentro de la universidad no se usa ningún tipo de firma digital, ni para mensajes internos ni para los externos ya que los comunicados de importancia no son enviadas vía mail si mediante oficio en papel.

En cuanto a la configuración de las estaciones de trabajo, no hay ningún control de acceso a sus sistemas BIOS, de manera que al momento del encendido de la máquina cualquier persona podría modificar sus opciones de configuración.

1.3 PASSWORDS

1.3.1 GENERACIÓN

Los password que existen en la universidad son generados en forma manual, sin procedimientos automáticos de generación. No tiene como restricción una longitud máxima ni mínima de caracteres, numéricos o alfanuméricos.
Cuando se da de alta un empleado en el sistema, su password se inicializa con el numero de cedula o del 1 al 6, advirtiéndole al usuario que lo cambie, pero sin realizar ningún control sobre la modificación del mismo.
Durante la auditoría pudimos comprobar que los password de acceso a los usuarios root a los servidores Linux no tenían tiempo de caducidad obligatoria.

1.3.2 CAMBIOS

Los cambios en los password los hacen los usuarios a través de la pantalla del login de Windows, allí hay un botón que muestra la opción para su modificación. Aunque generalmente los password no son actualizados por los usuarios, permaneciendo iguales por largos períodos de tiempo, ya que no tienen un plazo de expiración.

No se controla si el usuario utiliza siempre el mismo password, simulando cambiarlo pero ingresando nuevamente la clave que ha estado usando hasta ahora.

Si un usuario olvida su password, debe advertirle al administrador del sistema, el cual se resetea de manera manual e indicando cual es la clave puesta provisionalmente hasta que lo cambie el usuario. Al decírsela, no se requiere que el usuario la modifique, no se controla esta situación. Ocurre lo mismo cuando un usuario ingresa mal su contraseña dos o más veces seguidas el sistema no lo bloquea ya que puede intentarlo varias veces.

1.4 SEGREGACIÓN DE FUNCIONES

No se implementa ningún procedimiento o política para realizar la desactivación de usuario y clave cuando un empleado sale de vacaciones por varios días, más bien deja a pasantes su usuario y clave para que sean utilizados por ellos.

2 - SEGURIDAD DE LAS COMUNICACIONES

OBJETIVO DE AUDITORÍA: durante la Auditoría Informática se deberá evaluar la seguridad de las comunicaciones, los datos transmitidos, los dispositivos usados durante la transmisión, la documentación necesaria para la realización eficiente e ininterrumpida de esta transmisión, y los sistemas usados para la transmisión de datos de un entorno a otro, comprobando el cumplimiento de las normas de seguridad de la información.

2.1 TOPOLOGÍA DE RED

2.1.1 COMPONENTES DE RED

La red informática de la universidad se compone del siguiente equipamiento:

- 200 PC´s distribuidas entre las Unidades Académicas y Departamentos Administrativos,
- 12 Servidores, entre IBM, Hewlett Packard y PC clon:
  Ubicación: Edificio de rectorado
  Equipos:
  - Servidor web
  - Servidor de base de datos
  - Servidor LDAP
  - Servidor Proxy
  - Servidor de Cubos OLAP
  - Servidor de archivos

- Firewall
- Servidor DHCP
- Servidor de respaldos
- Storage
- Servidor DSPACE
- Servidor Telefonía IP

➢ 11 antenas de transmisión radial

NOMBRE	MARCA	MODELO	UBICACION
UNEMINET_ADMIN	D-LINK	2100AP	Departamento de Evaluación
UNEMINET_CCII	D-LINK	DWL-2100AP	Edificio de CCII, rack
UNEMINET_CCAA	D-LINK	DWL-2100AP	Edificio de CCAA, rack
UNEMINET_CCAA1	Tech Wise	CE 0560	Edificio de CCAA, planta alta
UNEMINET_CCEE	D-LINK	DWL-7700AP	Edificio de CCEE, Techo
CSIA	D-LINK	DWL-7700AP	Laboratorios, mástil
POSTGRADO	D-LINK	DWL-3200 AP	Postgrado planta alta
POSTGRADO2	D-LINK	DWL-3200 AP	Postgrado planta alta
UNEMINET_BIENESTAR	D-LINK	DWL-2100 AP	Bienestar, rack
UNEMINET_TICS	D-LINK	DWL-3200 AP	Edificio de rectorado, Tics
UNEMINET_BIBLIOTECA	D-LINK	DWL-3200 AP	Biblioteca

Tabla 21: antenas radiales de la UNEMI.

- 6 enlaces de fibra óptica
- cables UTP categoría 6,
- switch Cisco y D-Link:

EDIFICIO	DEPENDENCIA	EQUIPO	MARCA	MODELO
Rectorado	Tic - Data Center	Switch	Cisco	Catalyst 3560
Rectorado	Tic - Data Center	Switch	Cisco	Catalyst 3561
Rectorado	Tic - Data Center	Switch	Cisco	Catalyst 3562
Rectorado	Tic - Data Center	Switch	Cisco	Catalyst 3563
Rectorado	Tic - Data Center	Switch	Cisco	Catalyst 3564
Rectorado	Tic - Data Center	Switch	Cisco	Catalyst 3750
Rectorado	Tic - Data Center	Switch	D-Link	DES - 1024R

Tabla 22: Switch de la UNEMI

- Servidor soporte para telefonía sobre IP (próximamente las comunicaciones telefónicas internas de la universidad se desarrollarán con este método, usando la línea telefónica solo para las comunicaciones al exterior),

- Patch panel conectada a los switch central con entradas para PC's,

EDIFICIO	DEPENDENCIA	EQUIPO	MARCA
Rectorado	Tic - Data Center	Patch Panel	Siemon
Rectorado	Tic - Data Center	Patch Panel	Siemon
Rectorado	Tic - Data Center	Patch Panel	Siemon
Rectorado	Tic - Data Center	Patch Panel	Siemon
Rectorado	Tic - Data Center	Patch Panel	Siemon
Rectorado	Tic - Data Center	Bandeja de Fibra	Siemon
Rectorado	Tic - Data Center	Bandeja de Fibra	Siemon
Rectorado	Tic - Data Center	Bandeja de Fibra	Siemon
Rectorado	Tic - Data Center	Bandeja de Fibra	Siemon
Rectorado	Tic - Data Center	Bandeja de Fibra	Siemon
Rectorado	Tic - Data Center	Bandeja de Fibra	Siemon

Tabla 23: Pach Panel de la UNEMI

2.1.2 DESCRIPCIÓN DE LA RED

- **Enlaces radiales entre Edificios**: existe una conexión a través de enlaces radiales que conectan el edificio bloque “R” con el resto de los edificios para que tengan señal de internet, implementado con una topología de tipo BUS, ya que todos los puntos de conexión no pueden verse entre sí de manera de formar alguna otra topología más eficiente. Los datos viajan encriptados mediante un sistema de encriptación propio de las antenas dlink.

- **Fibra óptica entre edificios**: las conexiones entre los distintos edificios de la UNEMI se realizan a través de 6 canales de fibra óptica. Se implementó de esta forma debido a la corta distancia entre los puntos y a la alta velocidad requerida en el cable para los sistemas informáticos.
- **UTP en conexiones internas**: la totalidad del tendido de cables en el interior de la empresa se realizó con UTP categoría 6.
- **Switches**: los switches han sido programados para realizar un tipo de ruteo: direccionan los paquetes transmitidos por sector, según la dirección IP que traen, distinguiendo a que sector de la universidad van. De esta manera no repiten los paquetes de datos a toda la red, se disminuye el uso de ancho de banda y se evita la divulgación de los mensajes, mejorando la seguridad de la topología de Bus.

Se tiene acceso a Internet y a Internet avanzada mediante un convenio con la red CEDIA.

Las direcciones públicas IPv4 ofrecidas por esta red son:

- 190.95.144.25 ROUTER
- 190.95.144.26 MAIL UNEMI
- 190.95.144.27 WEB UNEMI
- 190.95.144.28 REPOSITORIO UNEMI
- 190.95.144.29 FIREWALL
- 190.95.144.30 CSIA UNEMI

Las direcciones IPv6 ofrecidas por esta red es la 2800:68:3::0/48

Existen 3 vlans para diferente uso en la UNEMI.

- Vlan de laboratorios: Sirve para conectar los dos edificios de laboratorios de la Unemi.
- Vlan inalámbrica: Sirve para conectar dispositivos inalámbricos en la Unemi. con acceso al Internet comercial y a la red avanzada.
- Vlan administrativa: Sirve para conectar las diferentes unidades. administrativas y académicas de la UNEMI.

2.2 CONEXIONES EXTERNAS

2.2.1 Edificios

La comunicación entre los diferentes edificios con el edificio de comunicaciones se lo realiza mediante fibra óptica y conexión inalámbrica.

La conexión de fibra óptica es utilizada para comunicarse entre los terminales con los servidores que están en el dpto. del TIC's.

La conexión inalámbrica es utilizada para tener internet en los equipos portátiles para consultas e investigación.

2.2.2 SERVIDORES:

Objetivo:

- Ofrecer servicios de red en la UNEMI.

Servidor web

	• **Objetivos:**	Proveer acceso a la página web de la UNEMI y permitir el envío y recepción de correo electrónico
	• **Ubicación:**	DATACENTER
	• **Marca y Modelo:**	HP PROLIANT ML370.
	• **Sistema Operativo:**	Linux Red Hat Enterprise 4.
	• **IP:**	190.95.144.27, 192.168.51.253,

Tabla 24: Servidor web

Servidor base de datos

	• **Objetivo:**	Proveer acceso a la base de datos de la UNEMI.
	• **Ubicación:**	DATACENTER
	• **Marca y Modelo:**	HP PROLIANT DL380G5

	• **Sistema Operativo:**	Linux Centos 5.2
	• **IP:**	192.168.51.1

Tabla 25: Servidor Base de Datos

Servidor de Preproducción y Desarrollo.

	• **Objetivo:**	Permitir acceso al servidor de pruebas de sistemas, antes de ingreso a producción.
	• **Ubicación:**	DATACENTER
	• **Marca y Modelo:**	HP PROLIANT ML370 G5
	• **Sistema Operativo:**	Linux Centos 5.2
	• **IP:**	192.168.51.150

Tabla 26: Servidor Preproducción y Desarrollo

Servidor base de datos web:

	• **Objetivo:**	Proveer acceso al servidor de base de datos para matrículas web y aula virtual.
	• **Ubicación:**	Administración, Planta Alta
	• **Marca y Modelo:**	HP PROLIANT ML370
	• **Sistema Operativo:**	Linux Centos 5.2
	• **IP:**	192.168.51.100

Tabla 27: Servidor Base de Datos Web

Servidor PDC, LDAP, MAIL

	• **Objetivo:**	Proveer acceso a perfiles y contraseñas para acceso personal de la Universidad. Proveer corre electrónico a personal de la Universidad
	• **Ubicación:**	DATACENTER
	• **Marca y Modelo:**	HP ML115
	• **Sistema Operativo:**	Ubuntu server
	• **IP:**	192.168.51.126, 192.168.51.254, 190.95.144.26, 192.168.50.253, 192.168.60.253

Tabla 28: Servidor Mail, PDC Y LDAP

Servidor proxy área de administración

	• **Objetivo:**	Permitir acceso a Internet
	• **Ubicación:**	DATACENTER
	• **Marca y Modelo:**	HP PROLIANT ML350
	• **Sistema Operativo:**	Linux Centos 5.2
	• **IP:**	192.168.51.252, 192.168.1.29

Tabla 29: Servidor Proxy

Servidor DHCP y Router

	• **Objetivo:**	Crear direcciones por DHCP para la red inalámbrica, y enrutar entre las diferentes redes de la UNEMI
	• **Ubicación:**	Laboratorios
	• **Marca y Modelo:**	IBM CLON
	• **Sistema Operativo:**	Linux Centos 4.1
	• **IP:**	192.168.51.251 192.168.52.1 192.168.53.1 192.168.54.1 192.168.55.1 192.168.56.1 192.168.200.1 192.168.100.1

Tabla 30: Servidor DHCP y Router

Servidor Firewall

	• **Objetivo:**	Proveer seguridad por medio del Firewall y control de contenidos de web.
	• **Ubicación:**	Laboratorios
	• **Marca y Modelo:**	IBM CLON
	• **Sistema Operativo:**	Linux Smootwall
	• **IP:**	192.168.99.1 192.168.6.1 190.95.144.30

Tabla 31: Servidor Firewall

Servidor Clientes livianos

	• **Objetivo:**	Proveer sistema operativo y acceso a la red a equipos ubicados en las aulas
	• **Ubicación:**	Biblioteca, 2 equipos
	• **Marca y Modelo:**	IBM X3550
	• **Sistema Operativo:**	Windows 2008 server
	• **IP:**	192.168.51.247 192.168.51.248

Tabla 32: Servidor Clientes Livianos

SERVIDOR DE TELEFONIA IP

El servidor de telefonía IP ofrece servicio de comunicación vía telefónica por medio de la red LAN de la UNEMI. Comunicación que cubre toda el campus de la universidad ya que existe red por toda la Universidad y también salida hacia fuera del campus UNEMI, ya que se conecta a la central telefonía Panasonic que tiene salida con líneas externas.

2.3 CONFIGURACIÓN LÓGICA DE RED

2.3.1 INTEROPERATIVIDAD WINDOWS - LINUX

Los recursos de Linux se comparten en la red de Windows usando una aplicación llamada **Samba**. Con esta aplicación, una porción del disco del servidor de aplicaciones se encuentra compartida con la red de Windows. Esto hace posible el entendimiento entre Windows y Linux, permitiendo a los usuarios de Windows acceder a datos que se encuentren en el sector compartido del servidor Linux, a través del Explorador de Windows.

El Samba tiene la capacidad de realizar autenticación, administrar perfiles, y demás opciones de seguridad de los recursos compartidos, donde se le establece un nivel de seguridad determinado a cada uno de los recursos de la red.

No todas las utilidades son usadas en la universidad, solo se utiliza el Samba como herramienta de comunicación entre los distintos sistemas operativos.

2.3.2 RECURSOS COMPARTIDOS

El entorno de red de cada uno de los usuarios está configurado para que le usuario no vea toda la red, sino solo una parte de la misma. Pero no hay ninguna medida tomada para que un usuario no comparta sus datos con otro usuario.

En la universidad, la configuración de esta aplicación no permite que haya visibilidad a las carpetas compartidas de los servidores, debido a que están en el área compartida del disco con la aplicación Samba, pero no disponibles para los usuarios en el Explorador de Windows.

En el área compartida del disco con la aplicación Samba se encuentran datos de la universidad (archivos indexados), las aplicaciones del sistema informático de la universidad (ejecutables). Los usuarios, desde Windows, acceden a los ejecutables de las aplicaciones a través de una aplicación de carpetas compartidas similar al Path de DOS, que direcciona al ejecutable, el cual tiene la propiedad de lectura, solamente. A través de éste camino, los usuarios pueden tener acceso a los programas en el servidor, de otro modo no sería posible, ya que el Explorador de archivos de Windows no tiene visibilidad sobre las carpetas del servidor.

2.4 MAIL

Todos los empleados tienen una cuenta de correo electrónico pero no todos necesitan este servicio, todos los Jefes de Área disponen de una, por este motivo esta vía de comunicación llega a todo el personal de la universidad, pero no existe control para el envío y recepción a correos externos. Este medio se utiliza para enviar todo tipo de información personal y del trabajo.

2.4.1 HERRAMIENTAS

La universidad cuenta con un sistema de mail interno. El interno está alojado en el servidor de correo de la universidad, y permite la comunicación entre el personal de los distintos departamentos. El mail interno tiene como dominio @unemi.edu.ec

El correo se lee con Outlook en las PC´s de la universidad. En el servidor se usa el SendMail, un administrador de correo de Linux, configurado por los técnicos de

Infraestructura encargados del mantenimiento, y gestionado por el administrador del TIC's donde está configurado el chequeo de la cuenta pop de cada usuario y avisa al usuario si ha arribado un nuevo mail, cada minuto.

2.4.2 ALTA DE USUARIOS DE MAIL

Si un empleado necesita una dirección de mail, porque su puesto de trabajo lo amerita, el Jefe del área al que pertenece le avisa al Director del TIC's, y éste delega al área de Infraestructura a que le asigna una casilla de correo.

Al momento de instalar el sistema operativo Linux por defecto en la instalación se crea la cuenta de administrador (root), para administrar todas las cuentas de todos los usuarios que tienen mail, debido a que para tener una cuenta de mail hay que estar definido como usuario en el sistema.

Cuando se genera una nueva cuenta de mail, el administrador del sistema (Coordinador Infraestructura) debe definir al usuario:

- en el servidor de hosting (LDAP),
- luego debe darlo de alta en el servidor de correo interno de la universidad (con el mismo nombre de usuario y la misma contraseña que usa para el ingreso a las aplicaciones de la Universidad),
- y por último el Outlook de la máquina del empleado.

En el momento de generar la nueva cuenta, el administrador le asigna un nombre de usuario a la nueva cuenta, de manera que los usuarios tienen conocimiento de sus password, ya que el administrador de Infraestructura u Operaciones los configura en el Outlook y allí se almacenan. Esto impide que un empleado utilice la cuenta de otro, ya que la única persona que conoce las contraseñas del administrador para instalar y configurar es Operación o Infraestructura del TIC's.

2.4.3 RECEPCIÓN Y ENVÍO DE MAILS

Cada minuto el SendMail chequea las casillas de correos del servidor de hosting. En el caso que exista algún mensaje nuevo, éste los baja al servidor de correo. El Outlook de las máquinas de los usuarios chequea el servidor de Correo cada minuto. Cuando actualizan sus bandejas de entrada, el mail es borrado del servidor y enviado a la máquina del usuario, sin quedar ninguna copia del mismo en el servidor.

En el caso del envío de mails, este no hace el mismo recorrido. La diferencia radica en que el mail interno no va hasta servidor de correo, sino que el SendMail identifica al destinatario y, si es un destinatario interno lo envía a la casilla interna. En caso de ser un destinatario externo lo envía directamente al ISP.

Los empleados no usan el mail solamente para funciones laborales, sino también con fines personales. Es posible ver los mail que se envían, pero actualmente no se realizan controles, de manera que pueden usarlo para cualquier fin. No se hace ningún control para comprobar si los usuarios se suscriben a listas de correo, no hay prohibiciones en este sentido.

2.4.4 CUOTAS DE DISCO

En el momento en que se crea un usuario de mail en el SendMail, se le asigna una cuota de disco del servidor de correo para los mensajes de entrada, con un tamaño de 10MB para cada usuario. No existe límite de tamaño para los mensajes de salida ya que no quedan almacenados en el servidor.

Si alguna de las casillas llega a los 10MB, entonces el SendMail manda un mail al usuario avisando que se está quedando sin espacio de disco, deja de recibir el correo y se bloquea la casilla.

No hay ninguna configuración especial para evitar el correo basura o mail bombing. Pero como las direcciones son locales, manejadas con servidores propios, no han ocurrido problemas en este sentido.

El servidor de mail no puede ser utilizado para enviar correo SPAM, ya que desde el firewall no se permite que un usuario externo envíe mails desde el servidor de la universidad.

Antivirus

El antivirus que está en el servidor de Internet chequea el mail, inspeccionando todos los mensajes entrantes y salientes, y sus archivos adjuntos. En el caso de

encontrar un mail infectado, se encarga de borrarlo, y el root envía un mail al destinatario del mensaje avisando que el mismo se eliminó.

Chat y Redes Sociales

Están restringidos el acceso a programas de chateo (generalmente el MSN). También están restringidos las páginas de redes sociales (ej: facebook y twitter). Esto se da porque los servicios que utilizan estos programas no están habilitados en el servidor por el consumo excesivo de ancho de banda que afecta a las operaciones y el buen desarrollo de la Institución.

Copia de seguridad

No se generan copias de seguridad de los mensajes, ni en el SendMail ni en el Outlook de los usuarios.

Privacidad – Firma digital – Encriptación de mails

No se utilizan firmas digitales ni encriptación en el correo electrónico. Algunos usuarios utilizan firmas de Outlook para enviar sus mensajes. No hay prohibiciones de envíos de información confidencial vía mail.

2.5 ANTIVIRUS

En la universidad no hay problemas con virus que sean considerados con un grado de peligro extremo o mediano; sin embargo hay una gran cantidad de PC´s con Windows XP infectadas con virus troyanos. No existe soporte de parte de Microsoft, para estos virus, los cuales no afectarón a los servidores Linux. Esta infección generó gran tráfico de red y congestionó la red. El problema se pudo controlar y erradicarse con el uso del antivirus Kaspersky servidor y cliente.

2.5.1 HERRAMIENTAS

En la empresa disponen de una versión corporativa del Kaspersky Antivirus, de manera que en el servidor de aplicaciones hay una versión para el servidor y en el resto de las PC´s hay una versión cliente de este antivirus. En el servidor de correo está instalado el Kaspersky Servidor 6.0 para el control de virus. El antivirus está ejecutándose continuamente y controla la recepción y el envío de mail, tanto en el servidor como en las PC´s. No hay discos de rescate o de emergencia del antivirus,

con los que se reinicia el sistema (bootea) desde DOS, el cual es usado para la restauración de máquinas infectadas.

2.5.2 ACTUALIZACIÓN

De Internet se actualizan las listas de virus del Kaspersky 6.0 a través del puerto de enlace (192.168.51.252), y el archivo ejecutable se almacena en una carpeta del servidor. El área de Infraestructura son los responsables de actualizar el antivirus y para esto fue configurado el Kaspersky para actualizarse apuntando a la última actualización bajada de Internet. No se hacen chequeos ocasionales para ver si se han actualizado los antivirus.

2.5.3 ESCANEOS DE VIRUS

No se hacen escaneos periódicos buscando virus en los servidores ni en las PC´s. No hay ninguna frecuencia para realizar este procedimiento, ni se denominó a ningún responsable.

2.6 FIREWALL

2.6.1 CONFIGURACIÓN DE SERVICIOS DEL FIREWALL

El firewall que existe en la empresa es un servicio del kernel de Linux, configurado de manera que se prohíben todos los servicios y solo se habilitan los necesarios (postura de negación preestablecida).

Se configuró en base a una política que discrimina tres clases de paquetes de red:

- los paquetes entrantes a la red,
- los paquetes salientes de la red,
- los paquetes en tránsito.

Por defecto, lo que no se habilite explícitamente está prohibido. Así se les va a denegar el acceso a todos los paquetes de entrada y a los paquetes en tránsito, mientras que a los de salida se les permite la salida. Algunas de las reglas más importantes son:

- Se aceptan todos los paquetes que van o vienen de la red interna, pero se les pone una máscara (con la dirección IP del servidor) para evitar que en el

exterior se conozcan las direcciones de red interna. Cuando vuelve la respuesta al paquete se le cambia la dirección nuevamente.

- Todos los datos que van dirigidas a un puerto 80 (HTTP), se re direccionan al Proxy.
- No hay restricciones a los puertos de salida.
- Se aceptan los mensajes loop back, para comunicación de la red consigo misma.
- Se aceptan los datos que entran por el puerto que se usa para la sincronización horaria en la red (servicios Date y Time).
- Se acepta el puerto 22, del SSH (Secure Shell).
- Los datos que están en tránsito son aceptados si provienen de la red interna.
- Se acepta el acceso de los puertos altos (son los puertos mayores al 1023): desde éstos puertos altos vienen todas las conexiones TCP/IP desde cualquier cliente externo. Es decir, cuando es necesario salir de la red, como un cliente, de un puerto local a un puerto remoto, el Linux asigna un puerto local alto. Así es que se deben permitir que ingresen datos desde los puertos altos, de otra manera no habría ningún paquete entrante.
- Se prohíbe el ingreso desde cualquiera de los puertos bajos, a excepción de los explícitamente permitidos (como el puerto 22, usado para mantenimiento).
- Los siguientes servicios no se encuentran deshabilitados explícitamente mediante reglas del firewall, pero no será posible acceder a ellos, salvo a través del SSH:
- No se deshabilitan los Shell y login, lo que significa que se puede acceder a los servicios remotos, como el RSHELL, REXEC y RLOGUIN.
- Está habilitado el TALK (que permite hacer un chat con otra máquina),
- Está habilitado el FINGER (que devuelve datos del usuario que está logeado en esa máquina, como nombre, estado, correo, etc.).
- Está habilitado el SYSTAT (que devuelve datos sobre el estado del sistema)
- Están habilitados los APPLETS y los SCRIPTS.

En el servidor de correo se encuentran habilitados permanentemente los puertos necesarios para el funcionamiento de la red y algunos servicios están deshabilitados y se activan solo cuando son necesarios, estos son llamados servicios on demand.

El SSH utiliza SSL (Secure Socket Layer) o sea una capa de servicios segura, en reemplazo de los servicios tradicionales. El mantenimiento de los servidores de la universidad se realiza a través de acceso remoto, usando SSH (Secure Shell), en reemplazo del Telnet por su seguridad ya que en SSH la información viaja cifrada y ante tres intentos fallidos de ingresar una contraseña corta la comunicación, mientras en el Telnet transmite en texto plano y no tiene restricciones de la cantidad de contraseñas que pueden ingresarse, facilitando el ataque de fuerza bruta.

2.6.2 TESTEO DE LA RED

El encargado de mantenimiento controla que los servicios permitidos sean los correctos, pero esta tarea la realiza sin ninguna frecuencia. Debido a que estas pruebas que se realizan no son formales, no se genera documentación alguna.
No hay evidencia de haber realizado pruebas de auto-hackeo, ni escaneos, ni intentos de intrusión o de escucha. Tampoco se hace un testeo periódico de puertos o de los servicios que están habilitados. Solo se revisan las instalaciones cuando hay quejas de los usuarios.

El firewall monitorea los intentos de ingresos, generando logs y mails por cada evento, pero no genera alertas de precaución (warnings) ante algún problema.
Además disponen del WebMin para monitorizar parámetros de la red, como el tráfico de red, aunque estos parámetros no son controlados con períodos determinados, ni se generan alarmas que alerten el trafico excesivo.

2.6.3 FALLA EN SERVIDORES

En el caso que haya algún problema con los servidores, se usaría el servidor de aplicaciones como reemplazo. Uno de los problemas que tienen el departamento TIC para levantar los servicios caídos, es no contar con servidores de respaldo es que no hay un servidor disponible, por lo cual hay que esperar hasta que este sea reparado.

En el caso que falle el firewall sería una falla segura, ya que los controles funcionan a bajo nivel (a nivel del kernel) y esta falla implicaría que el sistema operativo del servidor está inestable, de manera que nadie tendría acceso desde ni hacia la red externa (Internet).

2.6.4 PARCHES DE SEGURIDAD DEL LINUX

Las versiones del sistema operativo instaladas en los servidores son antiguas, por lo que casi no se consiguen actualizaciones. Esto puede repercutir en la seguridad de los servicios usados, como el SSH, generando nuevas vulnerabilidades.

2.7 ATAQUES DE RED

En la universidad no disponen de herramientas destinadas exclusivamente para prevenir los ataques de red, en principio debido a que no se han presentado, hasta el momento, problemas en este sentido.

Tampoco hay zonas desmilitarizadas ya que no se previene por falta de capacitación y por el nivel de costo que esto implicaría. Solo se dispone de un servidor firewall, por lo que hay datos publicados en línea (on line) desde el interior de la universidad que se debe proteger.

2.7.1 SISTEMA DE DETECCIÓN DE INTRUSOS (IDS - INTRUSION DETECTION SYSTEM)

En la universidad no se han registrado intrusiones, algunos intentos de intrusión que fueron impedidos por el firewall, pero no envió mails al usuario root del sistema operativo informando de los mismos.

No hay herramientas para detección de intrusos, solo cuentan con la configuración del firewall.

2.7.2 NEGACIÓN DE SERVICIO (DOS - DENIAL OF SERVICE)

No hay controles con respecto a la ocurrencia de Denial of Service. No existen herramientas que lo detecten, ni hay líneas de base con datos sobre la actividad normal del sistema para así poder generar avisos y limitar el tráfico de red de acuerdo a los valores medidos.

Disponen de una herramienta de monitoreo, que se ejecuta en una página HTML con datos sobre:

- tráfico de red,
- cantidad de archivos abiertos,
- cantidad de usuarios conectados a la red,
- uso de la memoria del servidor,

- uso del swap.

Además el kernel de Linux está capacitado para reconocer ciertos tipos de Denial of Service como TCP SYN Flood, Ping of Death, entre otros. De todas maneras el momento en el que Linux reconoce estos ataques es tardío ya que los canales de red ya estarán congestionados, y solo logra evitarse la congestión de los canales internos de la red.

2.7.3 SNIFFING Y SPOOFING

En la universidad la red se encuentra segmentada a través de switches, que efectivamente reducen la posibilidad de sniffing, ya que direccionan los paquetes de red de acuerdo al destino que tienen. Así se evita que el paquete viaje a través de toda la red o por destinos innecesarios.

Además los equipos de radio de la universidad encriptan los datos físicamente, por lo que el sniffing en estos tramos de la red resultaría más difícil.

No existe ninguna herramienta anti-spoofing. Como ya dijimos, el acceso externo está prohibido, debido a ser una máquina que funciona en modo cliente (no es un servidor de páginas Web), no obstante esto el firewall explícitamente deniega cualquier tráfico de la red externa que posea una dirección fuente que debería estar en el interior de la red interna.

2.7.4 ATAQUE A LOS PASSWORDS

El archivo de los password del sistema no se almacena en el directorio por default del Linux, en el /etc/passwd, aquí solo se almacena un archivo con los nombres y demás datos de usuarios. Este archivo está en texto plano y puede ser accesible ya que no está encriptado.

El archivo que contiene las password se encuentra en otro directorio, al cual solo el root tiene permisos para accederlo, éste es un archivo shadow, donde están encriptados. Se usa encriptación one way (en un solo sentido), de manera que no es posible desencriptar. En el momento del logeo, se encripta la contraseña ingresada por el usuario y se compara ésta contraseña encriptado con el dato almacenado que también está cifrado, si ambos son diferentes el logeo será fallido. Para modificar las

password, Linux accede a los datos simulando ser root, por lo que es posible la transacción.

3 - SEGURIDAD DE LAS APLICACIONES

OBJETIVO DE AUDITORÍA: La Auditoría Informática deberá evaluar la seguridad de las aplicaciones utilizadas en la universidad, la consistencia de sus datos de entrada y la exactitud de sus datos de salida, la integridad de las bases de datos y la existencia y el uso de la documentación necesaria para su funcionamiento, de acuerdo a los estándares propuestos.

3.1 SOFTWARE

En la universidad hay cinco servidores, con sistema operativo Linux y como resultado de una auditoría se eligió este sistema operativo por las siguientes razones:

- Porque necesitaban migrar a un sistema con entorno gráfico,
- Por el bajo costo (y la diferencia de precio con Windows 2000 Server),
- Por la confiabilidad,
- Por la compatibilidad que tiene con Windows (en el explorador de Windows se pueden ver las carpetas compartidas de Linux por el uso de un emulador),
- Por el buen control de acceso y la buena generación de logs de auditoría,
- Por la posibilidad de conseguir actualizaciones,
- Por el software de aplicación gratis,
- Por una experiencia mala con Windows,
- Por buenos consejos de profesionales capacitados.

Las aplicaciones en la universidad estaban desarrolladas en Visual Basic, Visual Fox 6.0, Fox 8.0 profesional y actualmente se están migrando a Web y Genexus. Hasta el momento esta reingeniería se encuentra en el 40% del desarrollo total de los sistemas. Los módulos de los sistemas que se han completado se encuentran funcionando desde el 2006 aproximadamente.

El 80% de las PC's usan el sistema operativo Windows 7, en el resto de ellas hay Windows XP. Usan software con licencia: Microsoft Windows y Microsoft Office, Kaspersky Antivirus, y demás utilitarios.
La página Web de la universidad no cuenta con un protocolo de sitio seguro otorgada por una entidad certificadora.

3.2 SEGURIDAD DE BASES DE DATOS

En la universidad se utiliza MySql para el desarrollo y la administración de datos, se almacenan la información de la universidad, tanto del area académico como administrativo; también hay tablas propias de fox que están guardados en una carpeta en un servidor de aplicaciones, donde se consultan valores recaudados anteriormente cuando los sistemas no estaban enlazados.

No se realizan controles de acceso lógico, a las carpetas donde se almacenen los archivos indexados, ya que estos archivos están en una carpeta del servidor no compartida para el resto de la red, a lo que se agregan los controles de seguridad física del servidor.

Las únicas personas que pueden tener acceso a la base de datos es el administrador de la base de datos y el administrador servidor de aplicaciones con sus cuentas de usuario respectivas.
Los aplicativos que administran la base de datos disponen de recursos suficientes para su funcionamiento, ya que aproximadamente solo el 60% de los recursos del servidor están en uso, el resto está libre.

Cuando algún usuario elimina registros de una base de datos, éstos no se borran físicamente, son marcados como deshabilitados; de esta forma siempre permanecen los registros de las transacciones realizadas.

3.3 CONTROL DE APLICACIONES EN PC'S

No hay estándares definidos, no hay procedimientos a seguir ni tampoco documentación respecto a la instalación y actualización de la configuración de las PC's. Solo hay una instalación básica de alguna versión del Windows, Internet

Explorer, Antivirus y una versión ejecutable de los sistemas integrador que son realizados por los desarrolladores del TIC's.

En el caso de que una PC presente errores en su configuración, se utilizan herramientas de reparación de errores, gratuitos, con el fin de evitar la reinstalación total del sistema y así causar una pérdida innecesaria de tiempo.
Tampoco se realizan actualizaciones de los programas instalados programados, como el Internet Explorer y el Microsoft Office. No se buscan paquetes de servicio o actualizaciones (Service Packs) ni nuevas versiones. La política de actualización de programas que se lleva a cabo permite actualizar los programas solo si es necesario debido a algún mal funcionamiento o nuevo requerimiento, lo que facilita la continuidad de los programas.

Las únicas versiones que se actualizan y quedan documentadas son las de los programas desarrollados por la universidad, a pedido de algún departamento. Estas versiones se actualizan directamente en el servidor, lo que evita hacer el control en cada una de las máquinas.

Solamente los administradores del TIC's son los encargados de las instalaciones en las PC's, porque los usuarios tienen restricciones con respecto a la instalación de programas. Pueden bajar de la web cualquier aplicación y no puede instalar en su PC porque está restringido por usuario.
Cuando se hace un cambio en la configuración del servidor, se guardan copias de las configuraciones anterior y posterior al cambio, pero no se documentan los cambios que se realizan ni la fecha de las modificaciones.

3.4 CONTROL DE DATOS EN LAS APLICACIONES

En las aplicaciones desarrolladas en la universidad se implementan controles en los datos de entrada (archivos y datos ingresados manualmente) y de salida, que aseguran su integridad, exactitud y validez.

Esto es controlado por el sistema Control de Acceso que maneja el Dpto. del ODI quien asigna los permisos de las opciones de los sistemas previa solicitud que le realizan los jefes de área.

Los equipos PC's de los usuarios están sincronizados con el servidor LDAP y de esta forma los logs y los datos siempre se generan con la fecha del servidor.

3.5 CICLO DE VIDA

La universidad cuenta con aplicaciones propias desarrolladas para cada uno de las áreas que la componen, por su grupo de programadores internos. Este desarrollo sigue una metodología estándar, que se usa la misma nomenclatura para denominar variables, tablas, parámetros, etc. Durante el ciclo de vida no se priorizaron los requisitos de seguridad del sistema, debido a la urgencia que envestía el proceso de reingeniería de sistemas y de puesta a producción de los mismos.

No se tiene definido el ciclo de vida de los equipos de computación (de 3 a 5 años de vida util), y de los sistemas informáticos (3 años de vida útil por obsolecencia tecnologica), se da de baja los equipos por daños generados por su uso.

Análisis: debido a que se trata de una reingeniería de sistemas, no se realizó un relevamiento formal para el desarrollo. Los programadores tenían noción de los requerimientos y necesidades de los usuarios por el conocimiento del sistema anterior; y a este se lo mejoró implementando nuevas funciones que demandaban los jefes de cada área.

Desarrollo: la implementación de los sistemas se está desarrollando bajo ambiente Web. Al comienzo del desarrollo se evaluaron las incidencias que podían representar los cambios en el sistema con respecto al sistema anterior, completándose así un análisis de riesgo preliminar. No se utilizaron herramientas, ni metodologías para evaluar factor hombres/horas estimado para el desarrollo de la pagina web.

Prueba: para el testeo del sistema se generan pruebas de uso, en un ambiente igual al de producción. Cuando se hacen modificaciones en los programas, las pruebas de uso sobre el software modificado son los mismos que se realizaron en anteriores ocasiones, de manera de comprobar que los valores obtenidos en las últimas pruebas sean los mismos que los que surgieron de las primeras. Las pruebas se realizan por módulos, y al integrar los módulos se realizan pruebas de integración.

Los resultados obtenidos en las pruebas son documentados en las carpetas relativas a cada uno de los módulos.

Instalación y modificaciones: una vez hecha la instalación, las únicas modificaciones que se realizan son a pedido del Jefe de área correspondiente, pero con la implementación de un formulario de solicitud de cambio. No se lleva a cabo ningún control de versiones ni gestión de configuración de las modificaciones.

Documentación: cada módulo desarrollado posee una carpeta con diagramas y documentación sobre el mismo. Se han desarrollado manuales para algunos casos, pero para otros no se han realizado, ya que la implementación de los mismos se han hecho aunque todavía no están realizados los manuales, para la totalidad de los módulos. Una meta del equipo de desarrollo es documentar el sistema en su totalidad, e incluso modificar los manuales existentes para generar un manual de usuario completo que englobe todos los sistemas de la empresa.

4 - SEGURIDAD FÍSICA

OBJETIVO DE AUDITORÍA: se evaluará que el TIC's, los equipos, los dispositivos, los medios de almacenamientos y las personas que conforman el sistema informático de la Universidad cumplan con las medidas necesarias en lo relativo a la infraestructura física y al mantenimiento de la seguridad de los recursos de la organización.

4.1 EQUIPAMIENTO

En sus principios contaban con equipos de poca capacidad pero al ir migrando a aplicaciones y sistemas operativos actualizados, se fueron adquiriendo PC clones con mayor capacidad, pero en la actualidad se está viendo la posibilidad de comprar equipos de marca como: HP, DELL, XTRATECH, etc., por su garantía ampliada y confiabilidad.

La universidad ha tomado la decisión de asegurar sus equipos informáticos y de red, debido al gran costo que implicaba y además llevar una parte del mantenimiento preventivo y la otra parte contratar un mantenimiento tercerizado permanentemente.

4.2 CONTROL DE ACCESO FÍSICO AL DPTO. DE TECNOLOGIAS

En el momento de la instalación del TIC's no se efectuó un análisis de costo-beneficio para determinar que controles de acceso físico sería necesario implementar.

Se está implementando un circuito cerrado de cámaras de video en algunas áreas de la universidad. Este sistema no es exclusivo del TIC's, ya que las cámaras están en toda el áreas de la UNEMI, ubicadas en puntos estratégicos, como en la puerta de ingreso, pero ninguna de éstas cámaras apunta al TIC's o a su puerta de ingreso.

La universidad cuenta con guardias de seguridad; en horarios laborales se ubican en el exterior del edificio Bloque "R" donde está ubicado el Dpto. TIC's y cuando se cierra la oficina, solo quedan en el exterior, además no cuenta con un sistema de alarma. El acceso al mismo es mediante código o huella digital, solamente cuando hay energía caso contrario no existe seguridad en su ingreso.

El personal que tiene acceso al Dpto. son los que laboran ahí, pero se ha visto que permiten el ingreso a estudiantes y personal de la Universidad, como a personas extrañas que realizan cierta actividad.

Siempre hay personal de sistemas en el interior del Dpto. TIC's, cualquier persona ajena a la oficina que necesite realizar una tarea de consulta, mantenimiento o limpieza deberá anunciarse en la puerta de entrada. El personal del TIC' es el encargado de escoltarlo desde la puerta hacia el interior de las oficinas del área respectiva, acompañándolo durante el transcurso de su tarea, hasta que sea concluida.

4.3 CONTROL DE ACCESO A EQUIPOS

Todas las máquinas de la empresa disponen de lectoras de CD y puertos USB, a pesar de que se está empezando a utilizar Internet o mail para el intercambio de información.

Estos dispositivos están habilitados y no hay ningún control sobre ellos, no se hacen controles automáticos de virus pero si se prohíbe el booteo desde estos dispositivos. Nunca hubo robo de datos usando medios externos, previniendo posibles fraudes ya que el usuario es el responsable de precautelar la información de sus PC's asignados.

Los gabinetes donde se ubican los switches de cada una de los edificios, están cerrados con llave, para evitar que el personal de limpieza o cualquier persona desconecten las entradas, y como medida de precaución, debido a que hay bocas libres en estos dispositivos. Las llaves de todos los gabinetes lo tiene a cargo el Coordinador de Infraestructura. Todos ellos están ubicados fuera del alcance del personal (a la altura del techo, o en espacios donde hay poca circulación de personal).

No se realizan controles periódicos sobre los dispositivos de hardware instalados en las PC´s, de manera que alguien podría sacar o poner alguno. Una vez que se ha completado la instalación de algún equipo, el administrador de Operaciones del TIC's no realiza chequeos rutinarios o periódicos, solo revisa los equipos ante fallas en los mismos, o por un problema reportado por el usuario.

Los servidores ubicados en el TIC's no se apagan en horarios no laborales, permanecen prendidos las 24 horas del día, aunque durante la noche no se realizan trabajos, permanecen ociosos, debido a que no existen procedimientos en lote (todos los programas se ejecutan on line).

4.4 DISPOSITIVOS DE SOPORTE

En el Dpto. TIC's disponen de los siguientes dispositivos para soporte del equipamiento informático: Aire acondicionado: la temperatura se mantiene entre 18ºC y 20ºC. Cuentan con un equipo de refrigeración central, y hay un equipo adicional de aire acondicionado de 24000 BTU, solo para esta área (cuarto de servidores), con el fin de mantener esta temperatura en invierno. Estas especificaciones las sugirió el personal que provee los equipamientos.

- **Matafuegos**: son equipos químicos, manuales y que fueron instalados por una empresa externa, donde se decidió que van a estar ubicados en el cuarto de los servidores.
- **Alarmas contra intrusos**: no cuenta con sistema de alarma en el departamento.
- **Generador de energía**: no cuenta con generador de energía ya que esto es un inconveniente que viene sufriendo en los constantes cortes de energía que sucede en la ciudad de Milagro.
- **UPS**: en el TIC's tiene un UPS que pueden mantener los servidores y las máquinas de desarrollo funcionando por 2 horas. Pero existe un inconveniente que también tiene salida de alimentación para el resto de oficinas del edifico por lo que disminuye el tiempo de soporte de energía a los establecido.
- **Estabilizador de tensión**: la corriente eléctrica proviene de un tablero independiente al que llega la línea de corriente externa, esta línea va a tres estabilizadores de tensión de donde salen tres líneas. Se dividió la carga eléctrica en tres sectores para un mejor funcionamiento:
    - Un sector abarca los equipos tecnológicos con UPS.
    - Otro sector es la parte que no tiene protección y luces.
    - La última corresponde a los aires acondicionados.
- **Descarga a tierra**: hay dos varillas de cobre que funcionan como descarga a tierra, una para el edificio y otra para el Dpto. TIC's.
- **Luz de emergencia**: no existe luz de emergencia que permanezca en carga las 24 horas del día y en el caso de un corte de luz se active automáticamente.
- **Piso falso**: el personal que proveyó el equipamiento sugirió poner un piso falso en el cuarto de servidores para que el cableado y conexiones se puedan manipular desde ahí.
- **Detectores de Humo:** son equipos que botan gas químico que luego es extraído, que fueron instalados por una empresa externa, donde se decidió que van a estar ubicados en el cuarto de los servidores para protección de los equipos.

4.5 ESTRUCTURA DEL EDIFICIO

Cuando se construyó el edificio del bloque “R” donde está ubicado el Dpto. del TIC’s, se tuvo en cuenta el diseño para el dpto. del TIC’s y sus condiciones de seguridad en parte. Por este motivo se lo ubicó en el sector posterior del edificio, para restringir el acceso. Está ubicado en un piso elevado, ya que en los piso inferior esta el área administrativa.

Las paredes externas del TIC’s son elevadas (aproximadamente 4 mts.) y las ventanas con vidrios oscuros que impiden la visibilidad desde el exterior del mismo.

El equipamiento informático fue provisto por una empresa que se encargó del asesoramiento técnico. A estos proveedores les consultaron cuáles eran los requisitos mínimos necesarios para que las garantías cubriesen los equipamientos (la instalación eléctrica necesaria, la refrigeración correcta del área, los métodos de aislamiento magnético, etc.) Para determinar qué medidas tomar en la instalación se realizó un análisis costo – beneficio donde se decidió, por ejemplo, implementar un piso falso en el Cuarto de servidores para el aislamiento, debido a que existía gran riesgo en las conexiones y el costo era muy elevado.

El Dpto. TIC’s fue diseñado pensando en su futuro crecimiento y actualmente sus instalaciones se encuentran convenientemente ubicadas, con la posibilidad de expandirse sin inconvenientes.

4.6 CABLEADO ESTRUCTURADO

La instalación del cableado fue tercerizado, y se implementó un cableado estructurado Cat. 6 blindado, brindándole a la UNEMI garantía de por lo menos de 5 años. Para diagramar los canales de red se tuvieron en cuenta los posibles desastres como inundación, cortes eléctricos, problemas de desagües o campos magnéticos.

Se implementó un techo falso, por donde tendieron el cableado, de fácil accesibilidad ya que se sacan los paneles que lo componen. Desde el techo falso los cables pasan por las columnas del edificio, y bajan hasta los perfiles de aluminio de los paneles que dividen las cajas, y por estos llegan hasta el suelo.

Estos paneles no son prácticos a la hora de hacer modificaciones en el cableado, debido a la cantidad de cables que pasan por ellos y al poco espacio con el que cuentan, pero resultaron económicos y son seguros en cuanto no es fácil desarmarlos. Por este motivo, y para facilitar la tarea de agregar cables en el interior de los paneles, hay tendido de cableado redundante que sí están conectados al switch del cuarto de servidores. En el resto de la red no hay entradas libres, ni puertos disponibles para poder instalar nuevas PC´s o equipos móviles.

En todo el trayecto del cableado se tuvo en cuenta la distancia mínima necesaria entre cables para no provocar interferencias, daños o cortes. Además no hay distancias grandes recorridas con cables UTP, para estas largas conexiones se utiliza fibra óptica o antenas radio que serian para conectarse entre los edificios.

Para que no haya interferencias se utilizó cableado UTP categoría 6 blindado, fibra óptica para conectar los edificios y antenas para cubrir con señal de internet todo el campus UNEMI. El mantenimiento de dichas antenas lo realiza una empresa externa.

Los cables en la patchera están numerados de manera que se los puede identificar fácilmente.
En cada toma hay un conector doble que tiene:

- 1 conexión UTP
- 1 conexión de teléfono.

Todas estas líneas no producen interferencias debido a la calidad de los cables de red, y a que la línea eléctrica está estabilizada. Además, la empresa encargada de la instalación de la red midió la interferencia que hay en las tomas de red de las PC´s encontrando que eran muy bajas y no representaban riesgos.

4.6.1 ANCHO DE BANDA DE LA RED

La empresa externa que instaló la red hizo una medición de la transmisión máxima que podía utilizarse, obteniendo un valor de 24 a 32 MB en el caso que se utilicen todos los recursos de red disponibles (esto es ejecutando la aplicación e Internet al

mismo tiempo). Este valor representaba un 70% de la capacidad de transmisión que garantizaba la empresa, ya que las antenas de transmisión tienen 8 MB de ancho de banda aproximadamente, de los cuales se garantizan 4 MB para la transmisión. Mientras que en el cableado hay UTP de 1 Gb.

4.6.2 FALLA EN LA RED

Por norma, cuando hay un corte de luz se activas los UPS, se graban los datos y se deja de trabajar en línea (on line). Si el corte supera la media hora de duración, entonces apagan los servidores como una medida de prevención.

En el caso de un corte en el servicio de red por falta de energía, falla en las antenas o en el switch, el área más crítica sería las unidades académicas que realizan matriculaciones o ingresos de notas en tiempo real.

5 - ADMINISTRACIÓN DEL CPD (Data Center)

OBJETIVO DE AUDITORÍA: los auditores deberán evaluar la correcta organización y administración del área de Base de Datos (Centro de Procesamiento de Datos), así como la asignación de tareas y responsabilidades del personal que la conforma; a fin de que ésta brinde condiciones óptimas de operación que posibiliten un ambiente adecuado de control y permitan mejorar la disponibilidad de sus servicios, de acuerdo a las normas existentes que regulan esta actividad.

5.1 ADMINISTRACIÓN DEL CPD (Data Center)

5.1.1 RESPONSABILIDAD DEL EQUIPO DE SISTEMAS

No hay responsabilidades puntuales asignadas a cada empleado, tampoco hay un encargado de la seguridad. Existe un responsable general de la Base de Datos, que es el administrador de la base de datos. Él es el que planifica y delega las tareas a los ayudantes. Además del administrador de la base de datos, hay una persona dedicada al mantenimiento de la página web de la universidad.

El administrador es el encargado de reportar al Director sobre las actividades en el área. Estos reportes generalmente se realizan a modo de auto evaluación o por pedido del director del departamento.

5.1.2 PLANES DE BASE DE DATOS

No se han desarrollado planes formales del departamento del TIC's hacia el área de base de datos, pues como prioridad principal es mantener el servicio del servidor de base de datos disponible las 24 horas del día.

La otra prioridad de esta área es el funcionamiento de la pagina web de la UNEMI como del aula virtual que es utilizado en la parte académica por los docentes de la universidad.

Luego se van asignando prioridades a las tareas a medida que surgen. No hay normas, estándares o procedimientos en las que se basen para la planificación, el control y la evaluación de las actividades del área.

5.1.3 IMPORTANCIA DE LA SEGURIDAD

Los empleados del área de la base de Datos tienen plena conciencia de la importancia de la seguridad que deben tener con la administración de la base, porque ellos son los que se encargan del buen funcionamiento de los sistemas cuando realizan consultas del mismo, aunque pudimos comprobar que no siempre cumplen las disposiciones de seguridad por no tener establecidos o plasmados en algún documento.

Clasificación de datos y hardware: los equipos de la universidad no han sido clasificados formalmente según su prioridad, aunque se puede identificar que las máquinas que están en el sector de atención al público tienen mayor prioridad que el resto. En la escala siguen las de los directores, y por último el resto de las PC´s, en cuanto al orden de solución de problemas. Si llega a haber un empleado esperando en alguna máquina, entonces esa es la PC que tiene la mayor prioridad en ese momento.

Informes Técnicos: hay procesos para realizar informes técnicos de las PC para manipular y dar de baja un equipo, sus periféricos o los medios de almacenamiento. Las máquinas y dispositivos se identifican entre ellas por medio de un registro de inventario que tiene cada equipo informático y además existe detalles suficientes para identificar sus características de compra y de garantías.

5.1.4 INTERACCIÓN CON EL USUARIO

Comunicación Institucional: normalmente los avisos informativos se hacen a través de mail, paneles informativos. Para el anuncio de una nueva norma o la modificación de un procedimiento existente, se emplea la misma metodología que en la capacitación a usuarios, con mail informativo y sala de reuniones.

Boletín informativo: en el dpto. de Tecnologías no utiliza un boletín informativo que se emita, cada vez que es necesario informar al usuario, o para recordarles las tareas de mantenimiento de sus equipos que deben realizar, como por ejemplo actualizar el antivirus, hacer copias de respaldo de sus datos, desfragmentar el disco, modificar y proteger sus password, borrar archivos temporales, entre otras.

Buzón de sugerencias: no han implementado un buzón de sugerencias donde los usuarios puedan expresar sus inquietudes.

5.1.5 INSTALADORES

Los instaladores de las aplicaciones utilizadas en la universidad se encuentran en sus Cd originales almacenados en porta Cd del departamento TIC's, y también disponen de copias para evitar posibles daños en los discos originales.

Los instaladores que son utilizados frecuentemente para la instalación en los equipos de computación de la universidad es el Antivirus Kaspersky, Windows 7 y paquete de office 2007, se ejecutan desde Cd copias de los Cd originales y pendrives.

5.1.6 LICENCIAS

En el Dpto. de Tecnología se mantiene un registro de los números de licencia de las aplicaciones instaladas en las PC´s y los servidores de la universidad. Los programas de los que se disponen licencias son los siguientes:

- Windows 7 y XP en las PC's.
- Microsoft Office 2007 en las PC's.
- Kaspersky Antivirus Corporativo.

- Fox 8.0 profesional
- Genexus 10.0
- Project y Visio 2007

El resto de las aplicaciones son propietarias, por lo que no necesitan de licencias, o son freeware como el Acrobat Reader y los Linux y Mysql en los servidores.

5.2 CAPACITACIÓN

La capacitación de los usuarios fue desarrollándose por áreas, a medida que se implementaban los distintos módulos de los sistemas académicos y administrativos. Cuando ingresa un empleado nuevo a la universidad se lo capacita en el uso del sistema, de la misma forma en que han sido capacitados los anteriores empleados: en la sala de reuniones del departamento del TIC's se le enseña el funcionamiento de los sistemas, aunque si el grupo de usuarios es reducido las capacitaciones pueden darse en el mismo sitio de trabajo de los empleados.

En estas capacitaciones se les instruye sobre consideraciones de seguridad como:

- no usar password fáciles de descifrar,
- no divulgarlas,
- no escribirlas ni guardarlas,
- entender que la administración del password es el principal método de seguridad del sistema.
- no modificar la configuración de las PC´s (configuración de red o del sistema).

Estas capacitaciones las da el administrador de Operaciones o el ayudantes de Operaciones asignado, generalmente los que trabajaron en el desarrollo del módulo hacen una presentación previa con los usuarios; una vez que han sido instruidos con una capacitación teórica, el personal de Operaciones se reúne junto con los usuarios en los puestos de trabajo, para asistirlos hasta que adquieran práctica, comprobando que el manejo del sistema sea el adecuado.

En ningún momento, hay consentimiento por parte de los usuarios a que auditen sus actividades en el sistema, ni declaraciones de que conocen las normas de "buen uso" del sistema.

5.3 BACKUP

5.3.1 BACKUP DE DATOS EN EL SERVIDOR

Cuando se hace un cambio en la configuración del servidor, se guardan copias de las configuraciones anterior y posterior al cambio, pero no se documentan los cambios que se realizan ni la fecha de estas modificaciones.

No hay ningún procedimiento formal para la realización ni la recuperación de los respaldos (backups). Además no se realizan chequeos para comprobar que el funcionamiento sea el correcto.
Los backups se hacen diariamente a última hora, después de las 8 p.m. Es un proceso que no está automatizado, por lo que todos los días, el encargado de la base de datos debe realizarlo, antes de irse, luego la comprime (zipea) y copia este archivo a una carpeta que va registrando los respaldos realizados.

Estos backups son incrementales, es decir que se agregan a la carpeta los archivos modificados y se backupea todo lo que ésta contiene. Debido a que se realizan estos tipos de backup incrementales, es imposible recuperar versiones antiguas de aplicaciones desarrolladas y luego modificadas, ya que se sobrescriben con las versiones nuevas.

Los sábados y domingos la universidad permanece abierta y se generan datos por medio de la pagina Web o usuarios que realizan horas extras en sus respectivos departamentos, y no se actualizan los backups hasta el lunes siguiente.
Para realizar el respaldo (backup) se utilizan discos compactos de 5 mm, uno para cada día de la semana; si el empleado encargado de los respaldos no asistiera a trabajar, no hay asignado ningún reemplazante, en ese caso el Director del TIC's delegaría a alguien esta responsabilidad.

No hay políticas de reemplazo de estos medios de almacenamiento, ni se les realizan controles para comprobar que están en buen estado y que su funcionamiento es el correcto.

El único responsable de realizar estos respaldos de la base de datos es el Administrador de Base de Datos y no hay ninguna política en cuanto a asignar un responsable para la restauración de los datos de los backups, esta tarea también la realiza el administrador.

Se han hecho pruebas de la recuperación de lo backups, cuando comenzaron con este procedimiento, y estas pruebas resultaron satisfactorias, pero no hay políticas de recuperación ni chequeos periódicos de este proceso. Los backups que se generan sobre las bases de datos han sido recuperados algunas veces por emergencias, obteniéndose resultados positivos.

5.3.2 BACKUP DE DATOS EN LAS PC´S

Los usuarios deben realizar sus propios backups de los datos almacenados en sus máquinas, ya que estos datos son propiedad de los empleados. Generalmente no los respaldan, debido a que los archivos que almacenen son de soporte o de poca importancia para la universidad.

Los usuarios han sido instruidos a almacenar los datos en la unidad “D” en la carpeta Mis Documentos que está configurado a esa unidad. Si hacen un backup deberían hacerlo en cd o pendrives.

5.3.3 BACKUP DE LA PÁGINA WEB

El administrador Base Datos realiza un backup de la página web completa en una PC que él tiene asignado, pero sin una frecuencia preestablecida.

5.3.4 BACKUP DE LOGS

No se hace ningún backup de los logs generados por las diferentes aplicaciones del servidor, solo se los almacena y se depuran semanal o mensualmente.

5.3.5 PROTECCIÓN DE LOS BACKUPS

Los archivos respaldados no están protegidos con ningún control de acceso ni encriptación. Esta situación puede resultar peligrosa ya que estos archivos contienen las bases de datos de la universidad y, ante cualquier incidente o extravío de los mismos, es fácil recuperar los datos en su formato original.

5.3.6 DOCUMENTACIÓN DEL BACKUP

No hay documentación escrita sobre los datos que se respaldan, dónde se hace esta copia ni datos históricos referidos a la restauración de los mismos.

5.4 DOCUMENTACIÓN

5.4.1 DOCUMENTACIÓN DEL TIC's

En el TIC's existe documentación sobre:

- Licencias del software, y en qué máquinas está instalado,
- Números IP de las máquinas y de los switches,
- Planos de la ubicación de los canales de red, desarrollados por el área de infraestructura que instaló la red,
- Gráficos de la ubicación física de los equipos.
- Inventario de insumos,
- Documentación del desarrollo de los sistemas.

No hay backups de ninguno de estos datos, ya que son documentos impresos que se van modificando manualmente.

5.4.2 MANUALES

No hay manuales de plan de contingencia a seguir, ni plan de continuidad. No se ha desarrollado ningún lineamiento de plan de seguridad informática, ni procedimientos formales sobre la seguridad de información.

Se comenzó a desarrollar manuales de usuario de los sistemas informáticos implementados, pero se completó solo un 60%, y actualmente están desactualizados.

Está en los planes del administrador de Operaciones del TIC's actualizar y terminar los manuales de usuario, explicando para cada módulo del sistema (o área de la universidad), el funcionamiento del mismo.

5.4.3 DOCUMENTACIÓN DEL DESARROLLO

Existe una carpeta con diagramas y documentación referente a cada módulo del sistema desarrollado, y allí se registran los cambios que se producen durante el uso del sistema.

Estos registros se generan durante las etapas de desarrollo y mantenimiento, pero no se actualizan los demás documentos o manuales cuando se hace una modificación del sistema, de manera que el cambio solo queda registrado en desarrollo.

6 - AUDITORÍAS Y REVISIONES

OBJETIVO DE AUDITORÍA: la Auditoría Informática debe evaluar las metodologías de control, auditorías internas y revisiones que se lleven a cabo en forma periódica, con el fin de encontrar debilidades y proponer mejoras, con base en las normativas que asesoran en el buen desempeño de la auditoría interna en la UNEMI.

6.1 CHEQUEOS DEL SISTEMA

6.1.1 HERRAMIENTAS DE GENERACIÓN Y ADMINISTRACIÓN DE LOGS

En la universidad, las siguientes aplicaciones o sistemas generan logs de auditoría:

- El kernel del sistema operativo de los servidores (Linux)
- El antivirus Kaspersky
- Servidor web
- Servidor de base de datos
- Servidor LDAP
- Servidor Proxy
- Servidor de Cubos OLAP
- Servidor de archivos
- Firewall
- Servidor DHCP
- Servidor de respaldos
- Storage
- Servidor DSPACE
- Servidor Telefonía IP

Cada una de las aplicaciones que genera los logs utiliza una carpeta diferente para su almacenamiento.

Para graficar los logs de auditoría se utilizan una aplicación llamada Monitor. Ésta lee los logs generados por las distintas aplicaciones cada cinco minutos, calcula las estadísticas y, cuando se llama al programa, grafica éstos valores. Este programa tiene la capacidad de no consumir gran cantidad de recursos.

Los procesos de rotación y eliminación de logs los realiza una aplicación llamada CronTab. Todos los registros se almacenan durante tres meses, y este programa se encarga de hacer la rotación mensual y eliminar los logs del mes saliente.

Los chequeos de logs se hacen manualmente ya que no hay una aplicación de administración de logs que genere reportes, ni hay alarmas en el sistema que avisen al administrador de la ocurrencia de un evento en particular.

Todos los logs contienen los siguientes campos:

- Fecha y hora
- Fuente (el componente que disparó el evento)
- ID del evento (número único que identifica el evento)
- Computadora (máquina donde se logeo el evento)
- Descripción (datos asociados con el evento o mensajes de error)

6.1.2 LOGS DE LOS SERVIDORES

El kernel de Linux monitoriza los servidores generando entre otros logs sobre:

- los servicios de mail,
- servicios de red,
- configuración,
- utilización del CPU,
- reinicio de servidores, entre otros servidores mencionados.

No se han buscado nuevas herramientas de generación ni gráfico de logs, por falta de tiempo.

6.1.3 LÍNEA DE BASE

Los valores que se recogen de los logs, son estadísticas generadas por el Monitor de red, en forma diaria, semanal, mensual y anual, con datos sobre tráfico de red,

cantidad de archivos abiertos, uso de memoria, uso del disco y uso del swap. Todos estos datos no generan una línea de base ya que no están almacenados como tal, sino que son datos estadísticos no persistentes calculados por el Monitor para realizar los gráficos.

Al hacer alguna modificación en la configuración del sistema, se genera una nueva compilación de datos (nueva línea de base), que no queda documentada. Esto se presta a confusiones, ya que no se identifica si ha habido algún incidente o si la variación se debe a cambios realizados en el sistema.

6.1.4 AUDITORÍAS INTERNAS

En la universidad no se realizan auditorías programadas, ni rutinas de chequeos de logs, debido a que no hay política para realizar controles, y solo se realizan cuando se presentan problemas o ante necesidades puntuales.

6.2 RESPONSABILIDADES DE LOS ENCARGADOS DE SEGURIDAD

El Director del TIC's o encargado por área:

- Administra, desarrolla e implementa los procedimientos de auditoría y revisión.
- Monitoriza y reacciona a los avisos (warnings) y reportes.
- Realiza chequeos aleatorios para verificar el cumplimiento de los requerimientos y procedimientos de seguridad.
- Revisa los reportes de auditorías o logs cuando es advertido de anomalías.

El encargado del mantenimiento de los servidores determina qué logs se generan, qué eventos de seguridad se auditan y qué datos se recogen. Además se encarga de buscar nuevas herramientas que faciliten la auditoría.

6.3 AUDITORÍAS DE CONTROL DE ACCESO

6.3.1 CONTROL DE ACCESO A LOGS

Los logs se almacenan en el servidor de aplicaciones o base de datos, por lo que cuentan con el control de acceso físico al servidor, pero no hay ningún control de acceso lógico a las carpetas donde están almacenados. Éstos pueden ser accedidos

desde cualquier máquina conectada a la red, conociendo la clave de administrador, a través del WebMin.

6.3.2 CONTROL DE ACCESO A INTERNET

Con respecto a las conexiones a Internet, existen registros con información sobre el número IP de la máquina conectada y la dirección de las páginas visitadas.

6.3.3 MODIFICACIÓN DE DATOS

El sistema operativo genera logs indicando qué datos se han modificado y en que momento, pero estos no son analizados por los administradores, solo se almacenan y se borran periódicamente. Existen logs sobre la mayoría de los movimientos de los usuarios en los sistemas de la universidad, generados y guardados en la base de datos. Esta aplicación genera reportes sobre qué máquina se logea, la hora a la que ingresa, a qué archivos accede y la hora a la que se desconecta, pero no contiene datos sobre el usuario que se está conectando.

Se piensa desarrollar un sistema de control de cambios para los datos, de manera que cada archivo del sistema de archivos indexados se asocie a una tabla de auditoría con las altas, bajas, modificaciones y consultas realizadas en los datos; pero esta aplicación todavía no está operativo.

6.3.4 CAMBIO DE PASSWORD

No se generan logs cuando un usuario modifica su password, no se guardan las contraseñas anteriores (para evitar la repetición), no se determina que aplicación se ha usado para realizar el cambio, ni en caso que el cambio resulte fallido, el motivo del fallo.

6.3.5 LOGS DEL ADMINISTRADOR

No se chequean periódicamente para verificar que sean válidos, que no haya habido intrusiones, o que no se registren ningún tipo de problemas.

6.3.6 LOGIN FALLIDO

El log generado no especifica el motivo del fallo, como por ejemplo si falló porque el password estaba mal, porque el usuario no existe, o porque tuvo dos intentos errados. Solo se identifica que hubo un error de conexión.

6.3.7 LOCKEO DE UN USUARIO

No existe lockeo de usuario, ni porque ingresó mal el password o usuario, y no se genera un registro de este evento, sino que el usuario debe avisar al administrador para que le ayuden en el ingreso.

6.3.8 PERFIL DE USUARIO

Con los logs que existen en la universidad sería posible generar perfiles de los requerimientos de cada usuario, pero no se hacen estas tareas, los datos se encuentran en bruto sin analizar.

6.4 AUDITORÍAS DE REDES

6.4.1 REPORTES DE CORREO

De los logs del mail no se calculan estadísticas, no se sacan **líneas de base** ni se grafican. El administrador solo los lee cuando supone que puede haber algún problema, a pedido de los usuarios por una supuesta falla en el servicio de mail. En el caso que se llene el espacio en disco de alguna cuenta, se envía un mail al root indicando el problema, pero no se emiten alarmas ni se generan logs.

El SendMail genera logs del tráfico de mails, aunque estos no se leen ni auditan. Estos logs se guardan durante 30 días, y se eliminan mediante la rotación de logs. En la oportunidad en que no se realizó la rotación correctamente, los logs del SendMail superaron los 4 GB de datos, por lo que fue necesario que el administrador los borre manualmente.

En estos logs se almacena el cuerpo del mail completo, pero no se guardan los archivos adjuntos, solo es posible consultar si contenía o no archivos, y los nombres de los mismos.

No se generan estadísticas sobre qué departamento o usuario de la empresa utiliza más el servicio de mail, o si a algún usurario le llegan más mail que la cantidad promedio, pero en los logs figuran los datos del usuario que sería necesario para realizar dichos cálculos.

6.4.2 ESTADÍSTICAS DE RED

Existen, como citamos anteriormente, gráficos sobre el tráfico en la red, proporcionados por el programa de administración de red denominado Monitor. Pero no existen datos detallados sobre el consumo de ancho de banda por terminal ni por sector de la empresa, de manera de tener la posibilidad de individualizar cuál de las terminales usa más tráfico de red o en qué parte de la línea el tráfico es más intenso.

Solo existen datos indicando la cantidad de bytes entrantes y salientes, pero no se detalla desde dónde se generan, ni con qué aplicación (mail, datos, aplicaciones, mensajes, Internet, etc.).

El Proxy utilizado (Squid) genera logs muy detallados, con datos sobre las páginas visitadas, el usuario, los horarios de entrada y salida, aunque no se generan reportes con datos relativos a los archivos descargados desde Internet. Esta aplicación tiene la capacidad de generar gráficos con los logs, aunque no se utilizan.

Tampoco existen reportes sobre las aplicaciones utilizadas por cada usuario, ni las prioridades de estas aplicaciones con el fin de discriminar qué cantidad de tráfico generan cada aplicación. Sería útil para ver qué aplicación usa más recursos, y restringir en el caso que sea necesario.

No hay datos estadísticos de los intentos de ataques. Cada vez que ocurre uno desde el exterior de la universidad, el administrador o encargado debe verificar y arreglar de manera inmediata para resolver el problema, sin documentar.

7 - PLAN DE CONTINGENCIAS

OBJETIVO DE AUDITORÍA: basándose en el análisis de riesgos desarrollado en la presente auditoría, se debe determinar cuáles son los activos con mayor nivel de

impacto y más vulnerables de la universidad, con el fin de asesorar en el futuro un posible desarrollo de un plan de contingencia y de continuidad de servicios críticos, teniendo en cuenta los riesgos más probables y considerando las distintas soluciones posibles.

7.1 PLAN DE ADMINISTRACIÓN DE INCIDENTES

En la universidad no hay planes formales para la administración de incidentes, como planes de contingencia, de recuperación de desastres o de reducción de riesgos tanto como hardware y software.

Actualmente las emergencias no está asignada a ningún personal del Dpto. de Tecnologías por lo cual la única persona responsable es el Director de Tecnologías.
Existen cuatro personas que están a cargo de sus áreas respectivas que se distribuyen las tareas a medida que se presentan las novedades, y esto se realiza sin ninguna planificación.

7.2 BACKUP DE EQUIPAMIENTO

7.2.1 EQUIPAMIENTO DE LOS SERVIDORES

En cada servidor existen 2 o3 discos duros con tecnología SCSI, donde cada uno de ellos tiene una capacidad de 1 Tera. Uno de ellos trabaja como disco raíz, un segundo disco funciona como disco espejo del primero, y el tercer disco es de respaldo (este disco no contiene datos).

Los servidores, ante una contingencia de daño, dejarían de funcionar hasta que se repare el mismo o pueda poner otro equipo de remplazo. Además se tiene respaldos de los servidores donde se podría adecuar otro equipo instalando y configurando según características del servidor dañado pero esto llevaría horas o 1 día realizar este acción, por lo que es perjudicial para la universidad no tener disponible el servicio que preste dicho servidor.

7.2.2 EQUIPAMIENTO DE RED

No hay backup de hardware debido a que no se ha proveído algún daño futuro en la red de la universidad, de manera tal que ante una contingencia física en algún

equipo, se estaría a esperas de reparar o comprar el dispositivo dañado. No se ha optado por la alternativa de asegurar la red o infraestructura de red de la universidad basándose en un análisis costo / beneficio que sería beneficioso para la UNEMI, teniendo en cuenta los costos de implementación, mantenimiento, entrenamiento técnico del personal, y de restauración en caso de una emergencia.

7.2.3 CPD ALTERNATIVO

Los datos de la universidad, del departamento TIC's y de todos los departamentos servidores se encuentran en el mismo cuarto de servidores, ya que no hay ningún centro de procesamiento de datos alternativo, porque no se previene tal daño o siniestro futuro.

7.3 PLAN DE RECUPERACIÓN DE DESASTRES

7.3.1 ACCIONES PREVENTIVAS

Constitución del grupo de desarrollo del plan

En el caso en que se genere un plan de emergencia de ataque de red, el encargado debe tener desarrollado o implementado un plan estratégico de cómo enfrentar un ataque de red, dada su función de Administrador de Infraestructura. En cada área del departamento TIC's existe un encargado, que son los que deben sugerir al Director las medidas de seguridad a implementar el plan que requiera su área.

Establecimiento del plan de acción

En caso de una emergencia de ataque de red es necesario tener desarrollado por lo menos dos planes de acción(acción A y B), para buscar, bloquear, neutralizar, enfrentar la intrusión al servidor de base de datos, que es el activo con mayor importancia. Debido que en él se encuentran los datos de todos los sistemas informáticos de la universidad. Todos estos planes de acción tienen los mismos objetivos proteger de un ataque de red.

Los activos más críticos a proteger serían:

- Datos:
    - Base de datos, datos almacenados en la base unemi, unemi net web, pago web, etc. documentación y de los sistemas.

- Programas fuentes y ejecutables de los sistemas de la universidad.

- Hardware:

- Servidores, switch central, equipos de radio, y canales de fibra óptica.
- Soporte físico de backups.

Definición de niveles críticos de servicio

Para precautelar la atención al cliente y la imagen institucional se debe definir los niveles críticos de servicio que son la conectividad de red, el ausentismo en la atención a usuarios dentro de la universidad y que tiene relación directa con el departamento del TIC's. En el caso que se demore o bloquee el servicio de datos, se detiene el servicio hasta solucionar el inconveniente, aplicando un manual de procedimiento o políticas de seguridad para prevenir un futuro desastre.

No se realizan simulaciones de siniestros para entrenamiento del personal, y tampoco la aplicación de las políticas de seguridad, solamente se realizaron al instalar los servidores, que se ejecuto un simulacro de sustitución de equipos, de esta manera que se comprobó su funcionamiento, pero se lo realizado de manera demorada.

7.3.2 PLAN DE CONTIGENCIA

No hay funciones definidas, para el personal del TIC's durante la ejecución de un plan de contingencia de desastres o robo de información. Las situaciones se resuelven a medida que transcurren, sin la aplicación de una política de seguridad informática a seguir, y además no se documenta las modificaciones e implementaciones de las acciones realizadas para enfrentar el desastre.

7.3.3 PLAN REACTIVA

Evaluación de daños

Se debe identificar las causas de las vulnerabilidades, una vez que ha ocurrido un ataque, los encargados de recopilar y evaluar los daños, deben presentar un informe al Director, quien evaluara los resultados obtenidos para la ejecución de alternativas de solución.

Ejecución de actividades

Una vez ocurrido el siniestro, el Director del TIC's ejecuta un plan de contingencia que debe estar elaborado previamente para salvaguardar los sistemas informáticos y data de la universidad, realizando las actividades de recuperación correctamente documentada, pero no se realiza este proceso de documentar las acciones y eventos ocurridos.

Retroalimentación del Plan de Acción

No hay un plan de acción a seguir, pero se toman acciones correctivas una vez que ha ocurrido un ataque de red de manera empírica, y no ponen controles activos de seguridad para que el mismo ataque no suceda a futuro. Una vez que han ocurrido los ataques no se realiza ninguna documentación con respecto a las modificaciones implementadas y a las acciones correctivas que se llevan a cabo.

INFORME DE PROBLEMA/INCONFORMIDAD Y RECOMENDACIONES A EJECUTAR

En este informe se presentan los problemas e inconformidades encontradas y las sugerencias que se deben implementarse ante la ausencia o la falla en los controles para el tratamiento de la seguridad de la información. Estas recomendaciones están avaladas por las normativas arriba enumeradas.

1 – RECOMENDACIÓN DE LA EVALUACION DE LA SEGURIDAD LÓGICA

1.1 ACCESOS

IDENTIFICACIÓN – ID

Problema o Inconformidad: durante la inspección se verifico que algunos usuarios no estaban asignados a un departamento de la universidad, dejando este campo, vacío en la base de datos.

Efectos: esta situación genera problemas en la identificación o asignación de permisos en el sistema de control de acceso. Esto genera una falla en la confidencialidad y posible divulgación de datos.

Recomendación: deberá tener en cuenta que no puede existir el valor NULL en el campo “grupo” de los datos de usuario, ya que de él dependen los futuros permisos que se le asignen.

Problema o Inconformidad: existen usuarios en el sistema para los cuales no estaba asignada una fecha de expiración del password.
Efectos: el problema de esta situación consiste en que el usuario no es obligado, en ningún momento, a modificar su clave de acceso, de manera que se facilita su revelación o robo.
Recomendación: el sistema no debe permitir que el campo donde se ingresa la fecha de expiación del password sea nulo, ya que de él depende el requerimiento de cambio de contraseña.

Problema o Inconformidad: cuando un usuario ingresa cinco o más veces mal la contraseña de ingreso, éste usuario no es bloqueado por el sistema.
Efectos: el usuario al modificar varias veces su contraseña, suele olvidar o confundir las claves (password), de manera que puede ingresar erróneamente la clave varias veces, lo que genera molestia.
Recomendación: el sistema resulta más eficiente si el número de intentos fallidos es cinco veces, así se genera un registro de bloqueos de usuarios y tener un mejor control de quien a ingresando con dicho usuario.

Problema o Inconformidad: no hay en la universidad un procedimiento formal para efectuar las bajas de registro de usuarios de los empleados en el sistema.
Efectos: los empleados próximos a desvincularse con la universidad o departamento TIC’s (cualquiera sea el motivo de esta situación) emprendan acciones de sabotaje, por rechazo o insatisfacción con esta decisión.
Recomendación: es conveniente que el área de recursos humanos de aviso al departamento del TIC’s, con un período de tiempo previo al despido, de esta manera es posible llevar a cabo una política de desvinculación del personal del sistema, a través de la cual se quitan permisos al usuario en forma periódica.
Con esto se disminuye el riesgo de robo o daño de información por insatisfacción con la decisión de la universidad.

Problema o Inconformidad: no se lleva a cabo ninguna revisión periódica ni control sobre el buen funcionamiento de las cuentas de los usuarios, ni sobre los permisos que tienen asignados.

Efectos: por error, negligencia, fraude o algún otro motivo, la cuenta o los permisos de algún usuario sean modificados, permitiendo que usuarios no habilitados accedan a datos que no le están permitidos.

Recomendación: Periódicamente sería conveniente controlar las cuentas de usuarios, viendo que:

- Estén activas solo las cuentas necesarias.
- No se han creado ni borrado cuentas.
- Los datos del usuario son consistentes.
- Los permisos que le corresponden son los que tiene asignados.
- Los password no están expirados y han sido cambiados periódicamente.

Problema o Inconformidad: no existe en el sistema una lista de control de acceso, esto imposibilita relacionar los usuarios con los datos que le es posible acceder, y qué permisos tienen sobre estos datos (lectura, escritura, modificación, borrado.)

Efectos: la ausencia de esta relación dificulta la trazabilidad de las acciones, de manera que resulta complicado identificar los permisos de los usuarios con respecto a los datos, archivos y carpetas del sistema, en el caso que sea necesaria una auditoría o revisión de la actividad particular de un usuario.

Recomendación: la generación de una lista de control de acceso donde se identifiquen a todos los usuarios habilitados en el sistema, los datos a los que pueden acceder y los tipos de permisos que los usuarios poseen sobre los mismos. Con esta herramienta sería posible personalizar perfiles de usuarios, que no dependan exclusivamente del grupo al que pertenecen.

Problema o Inconformidad: no se tiene en cuenta ninguna restricción horaria en el momento de permitir a un usuario la conexión (logeo) al sistema.

Efectos: este problema o Inconformidad puede permitir que un usuario no autorizado intente ingresar al sistema en horario no laboral (desde el exterior de la universidad, por ejemplo), condición que se ve agravada por el hecho que los servidores no se apagan, sino que permanecen prendidos las 24 horas del día.

Recomendación: debe restringirse el horario, en que pueden ser utilizados los sistemas informáticos de la universidad de manera que:

- las cuentas de los usuarios no deben poder acceder al sistema en horarios no laborales, de acuerdo al grupo al que pertenezcan (debido a que diferentes grupos pueden tener diferentes horarios).
- durante las vacaciones o licencias las cuentas de usuarios deben desactivarse.
- en días feriados las cuentas de usuarios deben permanecer desactivados.

Problema o Inconformidad: no se tiene en cuenta ninguna restricción con respecto al equipo desde donde se logea cada usuario.
Efectos: la falta de control, para identificar desde donde los usuarios acceden por la red desde un Pc, puede ocurrir que alguna persona no autorizada tenga acceso a un equipo que no le corresponde, permitiéndosele ver información para la que no tiene autorización.
Recomendación: se debe controlar la localización de los PC que se intenta conectar (logear), para así poder relacionar cada usuario con su propia PC, o con su propio grupo de trabajo

Problema o Inconformidad: aunque el usuario permanezca un largo período de tiempo sin actividad, el sistema no ejecuta ninguna acción; no se advierten a los usuarios sobre la necesidad de no dejar las máquinas logeadas e inactivas.
Esta situación pudo comprobarse también en los servidores, donde el administrador está logeado en el sistema permanentemente.
Efectos: el peligro en el que se incurre con esta debilidad radica en la posibilidad de que un usuario autorizado se conecte (logee) en el sistema y abandone su puesto de trabajo. Si otro usuario no autorizado tiene acceso físico a esta PC, éste último también tendrá acceso a datos que le están prohibidos. Esta situación se ve agravada si los equipos a los que se hace referencia son los servidores de la universidad, debido a que no solo se tiene acceso a datos críticos sino también a opciones de configuración de los sistemas.
Recomendación: si el sistema permanece sin actividad durante cinco minutos, el programa debería encargarse de desconectarse (deslogear) al usuario del sistema,

borrar la pantalla. Cuando el usuario regrese, se debería solicitar nombre de usuario y contraseña nuevamente.
Además, sería conveniente que las PC´s utilicen algún protector de pantalla con contraseña.
Estas recomendaciones se deben tener presente en la administración de los servidores.

Problema o Inconformidad: las cuentas de usuarios no pasan a un estado de suspensión, aunque permanezcan varios días sin actividad.
Efectos: persona no autorizada, tenga acceso a una cuenta de usuario que no le corresponde, permitiéndosele ver información para la que no tiene autorización.
Recomendación: Sería conveniente que el sistema, en forma automática, suspenda la cuenta de un usuario que no se logea durante cinco días. Además, si un usuario se va de vacaciones, o solicita una licencia, su cuenta debería inhabilitarse hasta su regreso.

Problema o Inconformidad: los servidores permanecen conectados (logeados) con el usuario root durante las 24 horas del día. De esta manera la seguridad de los datos del departamento y de la universidad que residen en el servidor solo dependerá del acceso físico al equipo.
Efectos: debido a que no hay controles lógicos, cualquier persona que consiga ingresar al TIC's podría acceder a los datos y a la configuración de los servidores.
Recomendación: el administrador solo debería utilizar este usuario del sistema en caso que fuera necesario realizar alguna tarea que así lo requiera. Para las demás actividades debería contar con otro usuario, con menos privilegios y por lo tanto menos riesgoso.

Problema o Inconformidad: los usuarios del sistema pueden tener abiertos, al mismo tiempo, todos los menús a los que están autorizados, y varias sesiones del mismo menú. No se hacen restricciones en cuanto a la cantidad de sesiones que los usuarios pueden utilizar.
Efectos: al abrir varias sesiones al mismo tiempo, existe la posibilidad que un usuario use la cuenta de otro para ingresar a los datos, complicando así la trazabilidad de las acciones de los usuarios. Además de no ser necesaria esta

posibilidad de tener varias sesiones abiertas, ya que con una sola sesión el usuario dispone de toda la información que necesita.

Recomendación: es necesario que solamente se pueda abrir una sesión de cada aplicación del sistema informático de la universidad, con el mismo nombre de usuario, y así no se podrán abrir dos sesiones del mismo menú en diferentes terminales, posibilitando esto el control sobre las actividades desarrolladas por los usuarios, a través de logs donde se registre el usuario, la terminal en la que está logeado y la aplicación que está usando. De esta forma se podrá identificar si en algún caso hay intentos de intrusión, o si simplemente se ha dejado logeada una terminal por error.

Problema o Inconformidad: en el Departamento hay cuatro personas con el mismo perfil de administrador, cada una de ellas tiene una cuenta diferente con un password determinado, pero a fines prácticos, los cuatro pueden modificar de tareas o instalaciones de la PC.

Efectos: con este esquema de acceso se imposibilita rastrear las acciones de cada uno de los administradores en el sistema, así no pueden asignarse responsabilidades individuales ante un posible error.

Recomendación: no es conveniente que varias personas accedan a la misma cuenta de usuario. Por este motivo sugerimos que cada uno tenga privilegios distintos de esta manera poder diferenciar a los cuatro administradores del sistema.

Debería existir un administrador total del sistema; y sugerimos que éste usuario esté en estado de inhabilitación, cuyo nombre de usuario y contraseña se encuentran guardados en un sobre cerrado.

El segundo en responsabilidad (un súper-usuario) tiene permisos iguales al anterior, con una restricción que lo imposibilita de borrar el usuario.

Además existiría una tercera cuenta de administrador, que tenga a su cargo un grupo de tareas de menor importancia y cotidianas del administrador.

En caso de que falte el administrador (el súper-usuario) por algún motivo, y el segundo requiera alguna tarea de mayor responsabilidad, este deberá recurrir a la cuenta, buscando los datos en el sobre. Una vez que esta cuenta ha sido usada, y el administrador retorna a sus tareas, deberá cambiar la contraseña de esta cuenta y guardarla en un nuevo sobre cerrado.

Problema o Inconformidad: el administrador puede logearse desde cualquier terminal de la universidad, además de tener la posibilidad de abrir varias sesiones del sistema al mismo tiempo.

Efectos: esta situación resulta riesgosa ya que el administrador podría dejar una terminal logeada con esta cuenta, lo que permitiría a cualquier usuario que acceda a esta terminal con perfil de administrador realizar cambios en los perfiles de usuarios y sus permisos, entre otras actividades.

Recomendación: Para evitar este desastre, el administrador debe poder logearse solamente desde ciertas terminales, las que se encuentren en el TIC's, y en una terminal específica y habilitada por cada edificio o departamento. Para poder realizar el mantenimiento del resto de las PC's sugerimos que se cree una cuenta. **mantenimiento** donde el administrador tenga permisos que le permitan realizar sus tareas habituales.

1.2 AUTENTICACIÓN

Problema o Inconformidad: una vez que algún usuario ha logrado logearse en el sistema se muestra solamente el nombre de usuario en la pantalla.

Efectos: si en una cuenta de usuario hubo un intento de intrusión, o se logró la intrusión, el usuario nunca se percatará de este ataque, como así tampoco lo hará el administrador del sistema.

Recomendación: en una pantalla intermedia se podría indicar, para un control personal del usuario, la siguiente información:

- Nombre de usuario
- Fecha y hora de la última conexión
- Localización de la última conexión (Ej. número de terminal)
- Intentos fallidos de conexión de ese ID de usuario desde la última conexión lograda.

  Esto es posible ya que toda esta información está guardada en los logs del sistema, pero no se los analiza. De esta manera el usuario puede llevar un control sobre sus conexiones.

Problema o Inconformidad: en cuanto a los mensajes externos desde la Dirección del TIC's hacia las otras Direcciones, que puede existir mayor importancia, podría utilizarse un sistema de firma digital.

Efectos: se reduciría la posibilidad de un ataque de Ingeniería Social o modificación del mismo, así como también contar con el beneficio del no repudio.
Recomendación: podría tenerse en cuenta la posibilidad de implementar un sistema de firmas digitales para así identificar fehacientemente al emisor; aunque esta recomendación solo sería conveniente en ciertos mensajes, aquellos que la Dirección considere de mayor importancia.

1.3 PASSWORD

Problema o Inconformidad: no se realiza ningún control sobre las cuentas de los usuarios, para comprobar que cambian el password asignado por primera vez.
Efectos: de ser así, el usuario permanecerá con un password fácilmente descifrable, facilitando la divulgación de esta contraseña y el robo de datos.
Recomendación: es necesario que, cuando el usuario se logea por primera vez al sistema, éste lo obligue a modificar su contraseña, impidiéndole el acceso hasta que éste procedimiento no haya terminado con éxito. Esto se logra ingresando la fecha de expiración del password como vencida en el momento de realizar el alta de un nuevo usuario.

Problema o Inconformidad: pudimos ver que el password de un usuario era un número fácilmente descifrable.
Efectos: al ingresar al sistema con un password fácilmente descifrable, es posible que los demás usuarios lo obtengan y accedan a datos que les están prohibidos.
Recomendación: Deberán considerarse herramientas para controlar que el password no sea fácil de descifrar, como puede ser realizar comparaciones contra una lista de palabras reservadas, por ejemplo el nombre de la universidad, el nombre de cuenta del usuario, números o letras repetitivas, entre otras. Una buena forma de crear un buen password es elegir una frase fácil de recordar y luego usar las primeras letras de sus palabras, por ejemplo: "La patria ya es de todos" puede formar el password “LPYEDT”.

Problema o Inconformidad: durante la auditoría pudimos comprobar que los password de acceso a los root de algunos servidores Linux son iguales.

Efectos: con una situación como esta se incrementa el riesgo de divulgación y robo de datos debido a que, si alguien tiene acceso al password del servidor de correo, también podrá acceder al servidor de LDAP con los permisos del administrador.
Recomendación: sugerimos que los password sean diferentes en ambos servidores, y que sean modificados con mayor frecuencia que los password de los usuarios.

Problema o Inconformidad: no se controla si el usuario cambia su contraseña ingresando siempre el mismo password, simulando cambiarlo, pero este ingresa nuevamente la clave que ha estado usando siempre.
Efectos: las contraseñas que no se modifican por largos periodos de tiempo corren el riesgo de ser descubiertas, debido a que seguramente habrá más oportunidades de descifrarlas.
Recomendación: deberá controlarse que el usuario ingrese una clave nueva cada vez que la modifique, así como que las últimas 5 claves no se repitan. Esto puede hacerse utilizando una base de datos donde se acumulen las últimas cinco claves que ha empleado cada usuario.

Problema o Inconformidad: generalmente, los password no son actualizados por los usuarios, permaneciendo iguales por largos períodos de tiempo, sin expiración.
Efectos: las contraseñas que no se modifican por largos periodos de tiempo corren el riesgo de ser descubiertas por más usuarios, debido a que seguramente habrá más oportunidades de descifrarlas.
Recomendación: consideramos que el período de vigencia del password no debería ser indefinido, suponemos que sería conveniente utilizar uno de 3 meses.

1.4 SEGREGACIÓN DE FUNCIONES:
Problema o Inconformidad: no se implementa ningún régimen de separación de tareas ni tampoco un sistema de rotación de personal en el TIC's o universidad.
Efectos: si un usuario tiene la capacidad (o los permisos) para realizar una tarea completa, pueden cometerse errores o fraude, sin que la irregularidad sea advertida. Al no haber una rotación de personal, es más difícil controlar la productividad del empleado, evitar posibles fraudes en el desempeño de sus funciones, así como el reemplazo del empleado en caso de su ausencia.

Recomendación: sería recomendable implementar un régimen de separación de tareas, para que un usuario no pueda realizar el ciclo de vida completo de una operación, y necesite de la intervención de otros empleados para poder concretarla, de manera que para poder realizar un fraude es necesaria la participación de más de un empleado, y se agrega un control para evitar posibles errores. Para esto será necesario restringir permisos a los usuarios.

Sería bueno tener en cuenta otro control, como la rotación de personal para controlar el desempeño que los empleados han tenido durante un período de tiempo. Además sirve para tener una persona capacitada de respaldo, en caso de necesitar una suplencia. Para poder llevar a cabo este control es necesario cambiar el usuario de grupo, modificándole sus permisos.

Estas tareas deberían estar a cargo del Departamento de Recursos Humanos, junto con los directores o con los responsables de cada área.

2 - SEGURIDAD DE LAS COMUNICACIONES

2.1 TOPOLOGÍA DE RED

No se hallaron debilidades significativas con respecto a este tema.

2.2 CONEXIONES EXTERNAS

Problema o Inconformidad: la comunicación con empresas externas que tiene vínculo con la universidad como bancos públicos y privados se realiza mediante internet y esta comunicación se realiza sin la supervisión del firewall.

Efectos: una conexión a Internet sin resguardo es peligrosa, ya que aumenta los riesgos de intrusiones, virus, entre otros sucesos no deseables.

Recomendación: es conveniente que se utilice un firewall en las PC's que utilizan conexiones a internet.

2.3 CONFIGURACIÓN LÓGICA DE RED

Problema o Inconformidad: existen carpetas compartidas en los servidores.

Efectos: al haber carpetas compartidas en el servidor pueden generarse intrusiones, robos de información o infecciones de virus.

Recomendación: no deberían existir carpetas compartidas en los servidores. Si es necesario grabar aconsejamos que el usuario tenga una carpeta compartida en su PC con una contraseña.

En cuanto a la carpeta compartida en el servidor, para actualizar el antivirus sugerimos que una vez que la actualización sea descargada de Internet se copie a otra máquina y desde allí se ejecute, o bien que desde Internet se baje directamente a otra máquina que no sea servidor.

2.4 MAIL

Problema o Inconformidad: al instalar los Outlook en las PC´s no se modifican las opciones de configuración por default, es decir que la vista previa y los controles ActiveX y Scripts están habilitados.

Efectos: la vista previa de los mails y la ejecución de controles ActiveX y Scripts son riesgosas ya que facilitan la infección con virus que se ejecutan automáticamente.

Recomendación: es conveniente exigir normas respecto a la habilitación y des habilitación de dichas características y la configuración mínima que debe poseer el Outlook en las PC´s. Debe deshabilitarse la vista previa de los mensajes y prohibirse la ejecución de controles ActiveX y Scripts.

Problema o Inconformidad: los empleados no usan el mail solamente para funciones laborales, sino también con fines personales. Actualmente no se controla el envío, pueden usarlo para cualquier fin. No se hace ningún control de que los usuarios se suscriban a listas de correo, no hay prohibiciones en este sentido.

Efectos: al utilizarse el servicio de mail indiscriminadamente se baja la performance de la red y se incrementa el riesgo de infección con virus.

Recomendación: debería controlarse que el servicio de mails se use solo para fines laborales, notificando a los usuarios de esta norma. Además sería conveniente hacerles advertencias con respecto a la suscripción a listas de correo.

Se podría calcular una estadística del nivel medio de tráfico de red generado por el correo electrónico, de manera que aquel usuario que sobrepase la media será evaluado para controlar si el uso que le da a este servicio es el correcto. De no ser así deberían tomarse las acciones correctivas respectivas.

Problema o Inconformidad: no se implementa un sistema de prioridades de mail.

Efectos: podrían mejorarse el envío de los mails a destinos como internas, bancos, y otros que merezcan mayor consideración.

Recomendación: el SendMail podría configurarse para que aquellos mensajes enviados por los Directores o los que tienen ciertos destinatarios, como externos, se envíen con prioridad alta.

Problema o Inconformidad: no se generan copias de seguridad de los mensajes.
Efectos: en el caso de una contingencia con el servidor de correos, los usuarios perderían los mails que no hayan leído hasta el momento del incidente.
Recomendación: podrían realizarse backups solo los mensajes con prioridad alta que se almacenan en el servidor de correos.

Problema o Inconformidad: no se utilizan firmas digitales ni encriptación en el correo electrónico a nivel de Dirección.
Efectos: sin la utilización de firma digital se puede correr el riesgo de ataques de ingeniería social.
Recomendación: podría utilizarse firma digital o encriptación para los mensajes con prioridad alta de las cuentas de correo de las Dirección, y así poder realizar un envío seguro al transmitir documentos confidenciales. Por ejemplo, podrían comprimirse la información de los mensajes para que no viaje en texto plano y protegerla con una contraseña para mayor seguridad.

2.5 ANTIVIRUS

Problema o Inconformidad: los usuarios son los responsables de actualizar sus propios antivirus.
Efectos: al no tener implantada una conciencia de seguridad, los usuarios no actualizan las listas de virus.
Recomendación: la actualización de las listas de virus debería ser responsabilidad del administrador de operaciones o un empleado del área de infraestructura designado por él. Éste debería, además, realizar chequeos aleatorios verificando que las listas de virus estén actualizadas y que se realicen periódicamente escaneos en busca de virus. Estas tareas deben realizarse tanto en las PC´s como en los servidores.

Problema o Inconformidad: no hay procedimientos formales a seguir en caso de infección de virus.

Efectos: al no utilizar un procedimiento como guía, puede ocurrir que el virus no sea eliminado completamente del equipo y se contagie a través de la red interna, además de la posibilidad de pérdida de datos en los equipos infectados.

Recomendación: debería haber un procedimiento documentado a seguir para el caso que se encuentre un virus en el sistema. Sugerimos las siguientes actividades:

- Chequear el disco con el escaneo de virus para determinar si hay un virus, y qué virus es. Eliminar el virus.
- Cerrar los programas, apagar la máquina y bootear la computadora desde el disco de rescate del antivirus.
- Hacer un nuevo chequeo de virus en el disco duro.
- Chequear el resto de los dispositivos de datos (disqueteras, disco removibles, etc.), para saber de dónde vino el virus.
- Tratar de determinar la fuente del virus. La persona que hizo llegar el virus debe ser informada.
- Avisar a todos los usuarios del sistema que hayan intercambiado datos con la computadora infectada.
- Si el virus borró o modificó algún dato, tratar de restaurarlo desde los backups y restaurar los programas involucrados.
- Hacer un nuevo escaneo del disco, buscando virus en los datos restaurados.

2.6 FIREWALL

Problema o Inconformidad: no se encuentran restringidos los servicios y protocolos que no son necesarios para el funcionamiento del sistema.

Efectos: esta situación genera una exposición innecesaria aumentando la probabilidad de ataques o intrusiones.

Recomendación: sería conveniente restringir más los accesos en el interior de la red. Los siguientes servicios no son necesarios y pueden desactivarse:

- El puerto 22 (de SSH) puede restringirse más habilitándolo on demand, y desde alguna PC determinada, la que se usará para el mantenimiento de la red. Se puede hacer lo mismo con el FTP, permitiendo su uso solo desde una PC en particular y en un horario determinado.

- Además sería conveniente deshabilitar definitivamente todos los servicios de puertos bajos no necesarios, que están habilitados desde el interior de la red, ya que no deberían utilizarse (como el TELNET).
- Es conveniente la utilización de herramientas de monitoreo de red. Puede ser conveniente la utilización de una aplicación (TCP WRAPPER) que habilita el uso de servicios como el FTP y el TELNET pero restringe el acceso de acuerdo a ciertas reglas de restricción, en función de la dirección (o el usuario) de origen. Así es posible permitir solamente que se utilice, por ejemplo el FTP, desde una determinada PC y con el fin de conectarse a las Unidades Académicas, con un destino fijo.

2.7 ATAQUES DE RED

Problema o Inconformidad: en el departamento del TIC's no disponen de herramientas destinadas exclusivamente para la detección de intrusos.

Efectos: al no haber un sistema de detección de intrusos instalado en los servidores, los atacantes tienen una barrera menos en el momento de ingresar a los datos en el departamento o universidad.

Recomendación: se debería usar algún sistema de detección de intrusos, estos deberían ser tolerantes al fallo, y ejecutarse con los mínimos recursos posibles.

3 - SEGURIDAD DE LAS APLICACIONES

3.1 SOFTWARE

No se hallaron debilidades significativas con respecto a este tema.

3.2 SEGURIDAD DE BASES DE DATOS

Problema o Inconformidad: los datos del departamento o universidad no se clasifican formalmente según su importancia.

Efectos: la clasificación de la información de acuerdo a su importancia permite asignar distintos niveles de controles de seguridad según la confidencialidad que sea necesaria, la falta de clasificación en los datos puede provocar la mala asignación de controles de acceso, y así posibilitar la divulgación de información.

Recomendación: sería conveniente que se clasifique la información del departamento o universidad, de acuerdo a la importancia de la misma, es decir teniendo en cuenta la confidencialidad y la disponibilidad que debe tener. Se podrían

definir tres niveles de información: crítica (la no-disponibilidad de esta información ocasiona un daño en los activos), confidencial (en poder de personas no autorizadas compromete los intereses de la institución) y pública (información de libre circulación). Esta clasificación ser documentada e informada a todo el personal de la organización, y deberá evaluarse y actualizarse periódicamente.

Problema o Inconformidad: a la información de la institución no se les asigna un responsable.
Efectos: al no haber un responsable encargado de la información, puede ocurrir que no se asignen los controles de acceso correctos, o alguien que responda ante los directivos en el caso de una contingencia (como puede ser pérdida o divulgación de información).
Recomendación: se recomienda asignar a la información un responsable, que asegure la confidencialidad, disponibilidad e integridad de dicha información.
En base a la clasificación enunciada anteriormente, el director del TIC's y el responsable de la base de datos deberían definir los controles de acceso a los datos.

3.3 CONTROL DE APLICACIONES EN PC'S

Problema o Inconformidad: no hay estándares definidos, no hay procedimientos a seguir ni tampoco documentación respecto a la instalación y actualización de la configuración de las PC's.
Efectos: al no haber estándares en cuanto a la instalación de un puesto de trabajo, puede realizarse una configuración equivocada, incurriendo en una pérdida de tiempo y productividad. Además puede ocurrir que cada empleado de operaciones del TIC's instale puestos de trabajo con una configuración diferente, lo que dificultaría el mantenimiento de los mismos.
Recomendación: sugerimos desarrollar un procedimiento formal a seguir cada vez que sea necesario instalar un nuevo puesto de trabajo en el departamento, o reparar alguna PC con errores de configuración, con el fin de establecer un estándar. Podría utilizarse, como complemento, alguna herramienta de restablecimiento y copia de configuración (como el Norton Ghost por ejemplo).
Sería recomendable documentar, no solo el procedimiento de instalación y reparación de puestos de trabajo, sino además cada uno de los mantenimientos que

se les realizan, a modo de historial de cada PC. Con esto se logra una documentación de la configuración actual de cada una de las máquinas.

Problema o Inconformidad: la ventana de comandos del DOS está disponible para todos los usuarios de Windows.
Efectos: esta aplicación posee una gran cantidad de herramientas peligrosas para la estabilidad del sistema, tales como el format o el deltree, que pueden ser ejecutados por usuarios inexpertos o maliciosos.
Recomendación: este comando (command.com) debería eliminarse de los sistemas Windows y en el caso que el administrador necesite de esta aplicación, podría utilizarla a través de la red o de un dispositivo externo.

3.4 CONTROL DE DATOS EN LAS APLICACIONES

No se hallaron debilidades significativas con respecto a este tema.

3.5 CICLO DE VIDA

Problema o Inconformidad: no existe un plan de desarrollo de sistemas formal, ni se utilizan métricas durante el ciclo de vida del software.
Efectos: al no tener un plan de desarrollo, puede ocurrir que se administren mal las prioridades, lo que implica un atraso en el desarrollo del sistema. Además, genera un despilfarro de recursos y una administración de tiempos generalmente deficiente.
Al no utilizarse métricas con el objetivo de cuantificar los pasos del desarrollo, la estimación de los recursos a utilizar puede desviarse mucho de la realidad, generando más problemas en el desarrollo.
Recomendación: sería conveniente que el equipo de desarrolladores siguiera un plan detallado, generado por el Director del TIC's o jefe de área, donde se definan las asignaciones de recursos, el establecimiento de prioridades, la administración de tiempos y la utilización de métricas de software, con el objeto de garantizar en forma eficiente el cumplimiento de las tareas propuestas.

Problema o Inconformidad: no hay políticas formales definidas para la contratación de terceros en el desarrollo.

Efectos: el tercero, al no tener conocimiento de las normas de seguridad implementadas en el departamento, puede no cumplirlas poniendo en riesgo la seguridad de los activos.

Recomendación: se debe informar por escrito la importancia de la seguridad de la información a todo el personal contratado, terceros y consultores. El Director del TIC's, junto con los jefes de áreas, deberían ser quienes especifican los requerimientos de seguridad, los pasos a seguir en caso que no se respete lo establecido en el contrato y piden al tercero en cuestión que informe posibles brechas de seguridad existentes.

Adicionalmente, los contratos con terceros deberían contener una cláusula que indique "Derecho de auditar" para asegurar que el personal de la empresa o las autoridades representativas puedan evaluar su desempeño.

4 - SEGURIDAD FÍ SICA

4.1 EQUIPAMIENTO

No se hallaron debilidades significativas con respecto a este tema.

4.2 CONTROL DE ACCESO FÍSICO AL TIC's

Problema o Inconformidad: no hay control de acceso físico al TIC's, ya que ninguna de las cámaras del circuito cerrado de video lo apunta a él o a su puerta de ingreso.

Efectos: al no haber un control de acceso especial en el TIC's, cualquier persona que tenga acceso al departamento y ante una distracción puede ingresar a al cuarto de servidores, con todo el riesgo que esto implica, debido a la sensibilidad crítica de los datos y activos que allí se encuentran.

Recomendación: sería conveniente que el departamento, donde se encuentran los servidores, el switch central y demás equipamiento crítico tenga una medida de seguridad extra, a través de la cual solo se permita el acceso a los administradores. Esto podría implementarse con una llave, ya que no implica mucho gasto y pueden darse copias solo al personal necesario. Ó, en reemplazo de esta medida, puede agregarse una cámara extra de video que grabe el interior del cuarto de servidores, o modificar la orientación de alguna existente hacia la puerta de ingreso al mismo.

Problema o Inconformidad: pudimos comprobar, durante la auditoría, que algún personal de mantenimiento de limpieza de la institución ingresó al TIC's y cuarto de servidores realizó sus actividades sin supervisión del personal del TIC's.

Efectos: esta situación puede resultar peligrosa ya que, como mencionamos anteriormente, en esta habitación se almacenan gran cantidad de equipos, corriendo el riesgo de robo de equipamiento o datos. Este incumplimiento de esta norma no ayuda a generar en los empleados una "cultura de la seguridad" sino que produce el efecto inverso, inseguridad.

Recomendación: cualquier persona ajena a la empresa que necesite realizar una tarea de mantenimiento en el TIC's y cuarto de servidores, debería anunciarse en la puerta de entrada. El personal del TIC's debería escoltar a los visitantes desde la puerta hacia el interior del departamento, acompañándolos durante el transcurso de sus tareas, hasta que éstas sean concluidas.

4.3 CONTROL DE ACCESO A EQUIPOS

Problema o Inconformidad: las máquinas de la empresa disponen de lectoras de CD y de USB, estos dispositivos están habilitados y no hay ningún control sobre ellos, no se hacen controles automáticos de virus ni se prohíbe el booteo desde estos dispositivos.

Efectos: debido a que cualquier usuario puede introducir un CD o pendrive con virus o intentar bootear desde estos dispositivos, esto implica un gran riesgo a la integridad del equipo y sus datos.

Recomendación: sería conveniente que las unidades lectoras de discos y usb se deshabilitaran desde el BIOS de cada máquina. Si llega a ser necesario, para realizar alguna tarea de mantenimiento, el administrador de sistemas puede ingresar al BIOS del equipo (utilizando la contraseña que él suministró), habilitar el dispositivo necesario y, una vez utilizado, deshabilitarlo nuevamente.

Problema o Inconformidad: no hay control de acceso a la configuración del BIOS de las PC´s y de los servidores.

Efectos: de esta forma al momento del encendido de la máquina cualquiera podría modificar las opciones de configuración de los equipos.

Recomendación: sería conveniente que las máquinas tuvieran configurado un password de administrador en el acceso al setup (BIOS), para evitar que se

modifiquen las configuraciones base de los equipos, esto podría aplicarse tanto a las PC´s como a los servidores. Estas contraseñas deberían gestionarlas el administrador de operaciones, en todos los equipos de la institución.

Problema o Inconformidad: no existe un control de acceso físico en el momento del encendido de los servidores.
Efectos: los servidores podrían ser encendidos por cualquier persona, sin que tenga que ingresar ninguna contraseña de ingreso.
Recomendación: sería conveniente que los servidores tengan implementado un sistema de llave de hardware, de manera que solamente el administrador, o la persona designada pueda encenderlos.

Problema o Inconformidad: no se realizan controles sobre los dispositivos de hardware instalados en las PC´s, una vez que se ha completado la instalación de algún equipo, el administrador de operaciones del TIC's no realiza chequeos rutinarios o periódicos.
Efectos: cualquier usuario podría sacar, poner o reemplazar algún dispositivo sin que se advierta la modificación.
Recomendación: sería conveniente que el administrador, o algún encargado de operaciones designado por él, realice chequeos periódicos para comprobar la correcta instalación de los dispositivos de los equipos, su buen funcionamiento y que sus números de series se correspondan con los datos registrados por el administrador al momento de la instalación.

Problema o Inconformidad: los servidores del TIC's no se apagan en horarios no laborales, permanecen prendidos las 24 horas del día, aunque durante la noche no se realicen trabajos, permanecen ociosos.
Efectos: al permanecer prendidos sin justificación, se acorta el tiempo de vida útil del hardware y se predispone a que se produzcan posibles intrusiones en el momento en que no hay nadie en el departamento para mitigar el ataque.
Recomendación: debido a que no es necesario que los servidores permanezcan prendidos las 24 horas, podrían apagarse automáticamente a las 22:00, horario en que se cierra la universidad.

4.4 DISPOSITIVOS DE SOPORTE

No se hallaron debilidades significativas con respecto a este tema.

4.5 ESTRUCTURA DEL EDIFICIO

No se hallaron debilidades significativas con respecto a este tema.

4.6 CABLEADO ESTRUCTURADO

No se hallaron debilidades significativas con respecto a este tema.

5 - ADMINISTRACIÓN DEL CPD

5.1 ADMINISTRACIÓN DEL CPD

Problema o Inconformidad: no se asignan responsabilidades puntuales a cada empleado en cada tarea, ni hay un empleado del TIC's como responsable de la seguridad de la institución.

Efectos: al no haber responsabilidades puntuales asignadas a cada empleado, pueden generarse malas interpretaciones con respecto a las tareas a desarrollar, lo que genera una pérdida de productividad.

Recomendación: deberían designarse responsabilidades claras y documentadas para cada empleado del TIC's, las que deberán constar en los procedimientos formales que se desarrollen para cada actividad. De acuerdo a las funciones que desempeñen deberán distribuirse los permisos particulares de cada uno de los usuarios en sus respectivas cuentas del sistema.

Además debería haber un empleado a cargo de la seguridad del sistema, que coordine las tareas relativas a este tema, haciendo cumplir las políticas de seguridad en todo el departamento.

Problema o Inconformidad: no hay, en los empleados del departamento del TIC's, plena conciencia con respecto a la importancia de la seguridad informática.

Efectos: al no existir una cultura de la seguridad implementada en el departamento, no se asegura el cumplimiento de normas y procedimientos.

Recomendación: a pesar de que existe una cierta conciencia sobre la seguridad de la información en la parte Dirección, el equipo del TIC's debe hacer hincapié en la concienciación de todos los usuarios, haciéndolos más responsables y partícipes de

las medidas de seguridad, ya que son los principales involucrados, tanto los usuarios actuales como los que se incorporen en el futuro.

Problema o Inconformidad: cada vez que los usuarios necesitan asesoramiento o servicios del TIC's se comunican telefónicamente con alguno de los miembros del área.
Efectos: no queda ninguna constancia de las tareas desarrolladas por los empleados del TIC's, ni de las solicitudes de los usuarios.
Recomendación: sería conveniente que los usuarios envíen mails al TIC's, solicitando asesoramiento o servicios, o para reportar incidentes o problemas con sus equipos, de manera que quede constancia de la misma.
Podría ser útil y eficiente la implementación de un buzón de sugerencias (por ejemplo una dirección de correo), donde los usuarios puedan recomendar mejoras o realizar cualquier tipo de comentarios, expresando sus inquietudes.

Problema o Inconformidad: no hay inventarios de los equipos de hardware, ni documentación con respecto a los equipos de la red física.
Efectos: esta documentación facilita las actividades de los administradores del TIC's, en el momento de realizar tareas de mantenimiento y para el desarrollo del plan de contingencias.
Recomendación: se debería implementar un inventario detallado de los equipos de cómputos, donde se incluya:

- Hardware: dispositivos instalados en cada máquina, número de serie, y demás datos sobre procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, cableado de la red, servidores, routers, etc.
- Software en los equipos: programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones, números de licencias, etc.
- Datos o principales archivos que contienen los equipos: durante la ejecución, almacenados en línea, archivados fuera de línea, back-up, bases de datos, dueño designado de la información, etc.
- Configuración de los equipos (y sus archivos de configuración).
- Ubicación de los equipos.

- Nivel de uso institucional de los equipos, etc.

Puede ser útil disponer de un responsable a cargo de la actualización del mismo, que controle periódicamente estos dispositivos y la información almacenada.
Sugerimos, además desarrollar procesos para rotular, manipular y dar de baja una computadora, sus periféricos y medios de almacenamiento removibles y no removibles.

Problema o Inconformidad: no se ha implementado un procedimiento que describa la manera de realizar la publicidad de las normas, directivas o modificaciones las mismas.
Efectos: en una organización es muy importante conocer las últimas modificaciones realizadas a los procedimientos o normas, de manera que nadie pueda excusarse de no conocer estos cambios.
Recomendación: debería existir un procedimiento describiendo la manera de realizar la publicidad de las modificaciones, incluyendo quién estará a cargo de la tarea. Esto puede llevarse a cabo mediante un mail, por exposición en transparencias, por notificación expresa, o por otra vía de comunicación.
Es fundamental tener en cuenta este punto ya que un gran porcentaje de los problemas de seguridad proviene del desconocimiento de las normas y/o modificaciones a ellas por parte de los usuarios.
Esta metodología deberá emplearse para el anuncio de la política de seguridad que se desarrollará y para sus futuras modificaciones.

Problema o Inconformidad: los usuarios deben realizar tareas de mantenimiento, como actualizar el antivirus, hacer copias de respaldo de sus datos, desfragmentar el disco, modificar y proteger sus password, borrar archivos temporales, entre otras.
Efectos: estas son tareas revisten gran importancia en el funcionamiento de los equipos de los puestos de trabajo, y una falla en su realización puede generar el mal funcionamiento de los mismos.
Recomendación: estas tareas de mantenimiento de las PC´s de los puestos de trabajo deberían ser llevadas a cabo por el administrador de Operaciones, o por alguien designado por él.

5.2 CAPACITACIÓN

Problema o Inconformidad: en ningún momento hay consentimiento por parte de los usuarios a que auditen sus actividades en el sistema, ni declaraciones de que conocen las normas de “buen uso” del sistema.

Efectos: no hay un aval de que el usuario ha comprendido las normas de buen uso del sistema, y que está dispuesto a cumplirlas.

Recomendación: una vez que el usuario ha sido capacitado en la realización de sus tareas cotidianas y tenga una clara visión del manejo del sistema se le podría comunicar la política de seguridad de la información y los procedimientos establecidos por la institución, además de un resumen por escrito de las medidas básicas, junto con una copia que debería ser firmada por él. Esto implica que está de acuerdo con las normas impuestas, y es consciente de las consecuencias que acarrea el incumplimiento de estas normas.

5.3 BACKUP

Problema o Inconformidad: no se documentan los cambios que se realizan en la configuración de los servidores, ni la fecha de estas modificaciones.

Efectos: al no tener documentación actualizada de los cambios realizados, se dificulta conocer la configuración exacta y actual de cada servidor, y de esta forma se obstaculiza la tarea del mantenimiento.

Recomendación: sugerimos que se documente cada uno de estos cambios, para así tener un control y una identificación de los mismos, así se podrá generar un historial de modificaciones y calcular estadísticas de los mismos, y con éstas será posible hacer más eficiente la configuración de los servidores.

Problema o Inconformidad: no hay ningún procedimiento formal para la realización ni la recuperación de los backups de los datos almacenados en los servidores de la institución.

Efectos: las copias de respaldo son el principal método de recuperación de datos del que dispone la organización y la ausencia de procedimientos para su implementación puede generar errores en el momento de un incidente.

Recomendación: consideramos necesario que exista un procedimiento escrito y formal de política de respaldo (Backup), que contenga las recomendaciones que se describen a continuación:

- Sería conveniente que el director del TIC's designe a un responsable de la realización de las copias de seguridad y de su restauración, y un suplente de éste primero.
- El procedimiento de generación de (Backup) debería estar automatizado con alguna herramienta de generación de copias de respaldo de datos.
- Las copias de respaldo deben realizarse en el momento en que se encuentre la menor cantidad posible de usuarios en el sistema.
- Debería realizarse un respaldo (Backup) incremental diario, todos los días de la semana, mientras que una vez por semana sería conveniente realizar un respaldo (Backup) completo de los datos más significativos.
- Deberían realizarse chequeos para comprobar que los procedimientos de restauración son eficientes.
- Los archivos de respaldo (Backup) deberían tener una contraseña que los proteja, o bien encriptarse, ya que contienen información confidencial.
- Los backups diarios deberían almacenarse en el exterior del departamento o Institución, ya que poseen un empleado designado, sería conveniente contar con un suplente.
- Sugerimos que este empleado se lleve el último Backup realizado, mientras que los demás CD's deberían permanecer en el interior de la Institución resguardados en un lugar ajeno al TIC's. Consideramos necesario que el CD que es llevado al exterior sea transportado en un medio resistente que lo proteja.
- Deberían realizarse chequeos para comprobar el funcionamiento correcto de los medios externos donde se realizan las copias de respaldo.
- Debería existir una política de reemplazo de CD´s, donde conste que deberían reemplazarse cada 6 meses, para evitar posibles fallas en el momento de la recuperación, debido al tiempo de vida útil del medio.
- Debería existir un procedimiento de recuperación de copias de respaldo, donde se incluya la metodología a seguir, quién tiene el permiso para realizarlo y en qué casos será permitido.
- Debería existir documentación de los backups generados, incluyendo:
    - ✓ qué datos contienen estas copias,
    - ✓ fechas de realización,
    - ✓ fechas de restauración,

- ✓ errores obtenidos,
- ✓ tiempo empleado en el proceso,
- ✓ demás datos que se consideren necesarios en la administración de este procedimiento.

Problema o Inconformidad: los usuarios hacen backups de sus datos en sus propias máquinas o pendrives.
Efectos: hacer un respaldo (Backup) en la misma máquina donde están los archivos originales no es garantía, y hacerlos en un pendrive tampoco sirve por la mala calidad del medio.
Recomendación: debido a que los usuarios no deberían tener habilitados dispositivos de almacenamiento externo lo más conveniente sería que el administrador de operaciones disponga de una máquina para la realización de backups. Allí debería generar todas las copias de respaldo de los datos de los usuarios. La carpeta donde se guarden estos backups deberá estar protegida con una contraseña gestionada por el administrador para restringir el acceso de otros usuarios.

Problema o Inconformidad: no hay ningún procedimiento formal para la realización ni la recuperación de los backups de la página Web de la institución.
Efectos: las copias de respaldo son el principal método de recuperación de datos del que dispone la institución y la ausencia de procedimientos para su implementación puede generar errores en el momento de un incidente.
Recomendación: debería existir un procedimiento formal de Backup de la página web, este Backup debe contener toda la página completa, y debe hacerse cada vez que se modifique la estructura de la misma. Este Backup debería almacenarse en el mismo equipo que los Backup de los usuarios, en otra carpeta protegida con contraseña.

5.4 DOCUMENTACIÓN

Problema o Inconformidad: no hay un buen soporte de documentación en el TIC's.
Efectos: al no poseer un buen soporte, la información puede ser incorrecta, inconsistente o desactualizada, lo que genera incertidumbre y dificulta la administración de incidentes.

Recomendación: sugerimos que la documentación posea mas detalles respecto a los siguientes datos:

- Diagrama de la distribución física de las instalaciones, identificación de PC´s y equipos, y puestos de trabajo
- Número de serie de hardware
- Número de licencia del software
- Inventario de "hardware" y "software"
- Fallas en equipos y trabajos de mantenimiento
- Entrada del personal externo.
- Configuración de equipos y servidores.
- Cambios en la topología de red.
- Modificaciones de emergencia realizadas a sistemas y hardware.
- Procesos estándares del Sistema Operativo (en especial de Linux sobre las operaciones básicas)
- Métodos para compartir datos entre sistemas (por ejemplo con las fábricas, entre las sucursales o entre las PC´s de la red).
- Toda esta documentación debería generarse teniendo en cuenta tanto la casa central como las sucursales.

Problema o Inconformidad: no hay desarrollados planes de seguridad, procedimientos formales, ni demás manuales o documentos de soporte para la gestión de la seguridad en la red informática.

Efectos: al no poseer un buen soporte, la información puede ser incorrecta, inconsistente o desactualizada, lo que genera incertidumbre en el momento de llevar a cabo procedimientos o procesos, lo que dificulta la administración general.

Recomendación: sugerimos que la documentación posea mas detalles respecto a los siguientes datos:

- Plan de contingencia
- Política de seguridad
- Manual de procedimientos
- Manual de usuario (del software y del hardware)
- Manual de seguridad para el sistema: detalla las funciones y privilegios de la seguridad. Contiene: configuración, administración y operación del sistema, guías para el buen uso de las características de protección del sistema, etc.

- Manual de seguridad para el usuario: asiste a los usuarios del sistema, describe cómo usar las protecciones, las responsabilidades de la seguridad del sistema.

Problema o Inconformidad: durante el desarrollo de sistemas, la documentación no es completa y las actualizaciones se realizan informalmente.
Efectos: por fallas en la gestión de la documentación pueden producirse errores en el desarrollo del sistema, así como una mala administración de recursos y falencias en la estimación de tiempos.
Recomendación: sugerimos la realización de los siguientes documentos para mejorar la documentación existente y así lograr una organización eficiente:

- objetivos,
- alcances,
- diagramas general y de funciones o de procesos,
- DER,
- diagrama de flujo,
- archivos de entrada-salida,
- responsable del módulo (analista que lo desarrolló),
- registro de modificaciones,
- lenguaje de programación,
- problemas o limitaciones conocidas,
- sectores de la Institución a los que afecta,
- descripción del "hardware" y "software" utilizados,
- características de seguridad,

Consideramos necesario que cada vez que se produzca una modificación en algún módulo del sistema, se modifique toda la documentación correspondiente. Las modificaciones deben hacerse de acuerdo a un procedimiento formal definido en la gestión de configuración.

6 - AUDITORÍAS Y REVISIONES

6.1 CHEQUEOS DEL SISTEMA

Problema o Inconformidad: no cuentan con una aplicación que genere alarmas o avisos cuando ocurre un evento que revista un determinado grado de riesgo.

Efectos: para que el administrador tome conocimiento de la ocurrencia de algún incidente problemático, debe leer los registros generados por las aplicaciones, analizarlos y tratar de encontrar problemas en un gran archivo de textos. Esta situación no resulta práctica, y puede ocurrir que la notificación del problema llegue tarde, cuando el error ya está avanzado.
Recomendación: aplicación para generar reportes y alarmas, ya que la lectura de los logs es tediosa y poco práctica, sería conveniente generar alarmas o algún otro mecanismo de alerta cuando ocurra algún evento en particular. Usar una aplicación que administre los logs, teniendo en cuenta la severidad de los eventos, e identificando el usuario asociado al evento.

Problema o Inconformidad: no se buscan nuevas herramientas de generación ni gráfico de logs.
Efectos: puede perderse efectividad y eficiencia con el uso de herramientas poco prácticas y desactualizadas, que no poseen generación de reportes ni alarmas, para que el administrador esté siempre al tanto de las situaciones riesgosas.
Recomendación: sería conveniente actualizar continuamente las herramientas que se usan para graficar la información generada en los logs. Debería asignarse la responsabilidad de esta tarea a una persona específica.

Problema o Inconformidad: no existe una línea de base definida, solo disponen de los datos almacenados en los logs.
Efectos: no es posible comparar medias o promedios generados en la institución en situaciones normales con los valores actuales obtenidos de los logs, e identificar actividades inusuales.
Recomendación: sería conveniente generar líneas de base, en vez de un conjunto de datos históricos, para poder tener información sobre las PC´s, los servidores y el sistema en general con detalles sobre, por ejemplo:

- qué usuario, sector o tarea utiliza más recursos de CPU (para calcular este dato dispongo de los logs generados por el servidor),
- qué datos son los que consumen más tráfico de red, memoria o CPU,
- qué datos se utilizan o se modifican con mas frecuencia.

- qué archivos tienen mayor índice de crecimiento (en los logs que genera el Servidor hay información sobre quién accede a cada dato, en que momento accede y en qué momento libera los archivos),
- qué aplicaciones son más utilizadas,
- qué aplicaciones consumen más recursos,
- quién utiliza más memoria del servidor,
- en qué momento surgen cuellos de botella y en qué recursos,
- en qué momento o por cuánto tiempo la memoria o el CPU permanecen usados en un 100% de su capacidad.

Problema o Inconformidad: los logs se eliminan sin generar un Backup de sus datos.
Efectos: al no hacer Backup de los datos de los logs no es posible obtener datos estadísticos para la generación de las líneas de base.
Recomendación: sería recomendable, antes de eliminar los logs, generar un resumen de líneas de base y estos resultados guardarlos en CD's.

Problema o Inconformidad: en el TIC's no se realizan auditorías programadas, ni rutinas de chequeos de logs.
Efectos: al no realizar controles aleatorios resulta difícil verificar el cumplimiento de los requerimientos y procedimientos de seguridad.
Recomendación: sería conveniente que se programen auditorías y chequeos aleatorios, para controlar las áreas o funciones críticas con respecto a la seguridad de los datos de la institución, documentando la ejecución y los resultados de dichas pruebas.
Debe tenerse en cuenta la recomendación sobre separación de tareas, ya que la persona que realice dichas revisiones no debería estar comprometida con la tarea a auditar. Además, si el tamaño de la auditoría lo justifica, sería conveniente que la lleve a cabo un grupo de dos o más personas, para disminuir las tentativas de corrupción.

6.2 RESPONSABILIDADES DE LOS ENCARGADOS DE SEGURIDAD

No se hallaron debilidades significativas con respecto a este tema.

6.3 AUDITORÍAS DE CONTROL DE ACCESO

Problema o Inconformidad: la información que se almacena en los logs con respecto a las conexiones a Internet no es suficiente, ya que solo se almacena el número IP de la máquina conectada y la dirección de las páginas visitadas.

Efectos: al no disponer de la información necesaria, no será posible conocer las actividades de los usuarios en la red, como por ejemplo identificar la procedencia de posibles virus.

Recomendación: sería útil poseer información más detallada sobre:

- Cookies guardadas
- Archivos descargados
- Servicios utilizados
- Aplicaciones utilizadas

Problema o Inconformidad: no se identifican los usuarios que acceden a datos.

Efectos: no se puede identificar qué usuario accede a los datos, debido a que no se tiene información sobre la máquina que ingresa al sistema solo se obtiene del usuario que accede a los datos y cualquier usuario podría utilizar cualquier máquina.

Recomendación: es conveniente que se identifique la maquina por la que acceden los usuarios a los datos y así será posible rastrear las acciones de cada usuario en el tiempo.

Problema o Inconformidad: no se generan reportes relativos a las actividades de los usuarios sobre los datos.

Efectos: para el administrador del sistema resulta muy complicada la revisión de las actividades de los usuarios basándose en un estudio de los logs, debido a la cantidad de tiempo que implica esta tarea.

Recomendación: podría utilizarse una herramienta de generación de reportes de manera automática con datos sobre:

- Cantidad de usuarios que acceden simultáneamente a la base de datos (cantidad de conexiones activas),
- Estadísticas de entrada-salida para cada usuario,
- Tiempo y duración de los usuarios en el sistema,
- Usuarios que no han ingresado al sistema por un largo período de
- tiempo.

- Generación de nuevos objetos de bases de datos,
- Modificación de datos,
- Número de intentos fallidos de conexiones a bases de datos.
- Se deberán generar estadísticas o líneas de base de estos datos, a fin de utilizarse para el control de los datos de la base de datos.

Problema o Inconformidad: no se realizan chequeos periódicos a los logs generados con el usuario administrador del TIC's.
Efectos: al no generarse reportes sobre las actividades del usuario administrador, se corre el riesgo de que algunas acciones de intrusos o no permitidas pasen inadvertidas.
Recomendación: deberían realizarse controles sobre estos logs, comprobando que las acciones realizadas por el administrador se correspondan con los datos que en ellos figuran, de manera de identificar posibles intrusiones o anomalías.
El estudio de estos reportes no debería ser realizado por el administrador, sino por el Director o jefe. Para que esta recomendación tenga validez, deberá cumplirse la sugerencia que imposibilita a los usuarios y administradores la modificación de los logs.

Problema o Inconformidad: no se generan logs cuando un usuario modifica su password.
Efectos: deben poder rastrearse todas las actividades del usuario en el sistema.
Recomendación: sugerimos que se generen logs cuando un usuario modifica su contraseña, agregando datos como la aplicación desde la que se realizó el cambio y en caso que el cambio resulte fallido, el motivo del fallo.

Problema o Inconformidad: los logs generados por un login fallido no especifica el motivo del fallo.
Efectos: al no incluir el motivo del fallo en los logs, no será posible determinar si hubo un error en el sistema, intento de intrusión o el usuario confundió su contraseña, entre otras.
Recomendación: detallar el motivo del login fallido en el contenido del log.

Problema o Inconformidad: no se generan perfiles de los usuarios con respecto a sus actividades.
Efectos: sin estos perfiles no se pueden identificar anomalías por grupos de usuarios.
Recomendación: sería conveniente generar estos perfiles con el objeto de saber que uso le dan a Internet, el tráfico de mails, tráfico de red que genera cada usuario o área del TIC's o institución, que terminales utilizan, las horas de acceso, etc., para así determinar qué acciones son inusuales y deban ser investigadas.

Problema o Inconformidad: no se generan logs cuando se requiere una impresión de algún dato suministrado por los sistemas de la institución.
Efectos: al no generar logs no se tiene un control sobre los datos del departamento o institución impresos, ni de los usuarios que solicitan esta tarea.
Recomendación: cuando un usuario solicita una impresión de algún dato de los sistemas de la institución, debería generarse un log de dicho evento.

6.4 AUDITORÍAS DE REDES

Problema o Inconformidad: no poseen un plan de monitorización general de la red.
Efectos: al no tener un plan organizado de monitorización, puede ocurrir que baje la performance del sistema debido a cuellos de botella en los recursos.
Recomendación: generar un plan de monitorización, teniendo en cuenta que la monitorización tiene un impacto directo en la performance del sistema. Se podría utilizar, por ejemplo, alguna herramienta para monitorizar el tráfico y rendimiento de red, como un escáner de seguridad integral.

Problema o Inconformidad: no se auditan regularmente ni se generan estadísticas sobre los logs referentes al correo electrónico.
Efectos: al no tener estas estadísticas no se calculan ni se grafican líneas de base y al no realizar monitoreos periódicos no se puede alertar al administrador sobre anomalías o posibles errores.
Recomendación: el administrador o un encargado del área de Infraestructura TIC's debería ser responsable de la monitorización de éstos logs, generando reportes diarios o mensuales, con los siguientes datos:

- poco espacio libre de cuotas asignadas al correo,

- disminución en la performance del correo,
- demasiados mensajes entrantes o salientes fuera de lo normal,
- departamento o usuario de la institución que utiliza más el servicio de mail,
- warnings o advertencias ante la aparición de un virus,
- estadísticas sobre mails infectados con virus, períodos de mayor infección, máquinas más afectadas, direcciones fuentes qué mas mails infectados envían, cantidad de archivos infectados por extensión (Ej. Los archivos de Word se infectan más que los de Excel),

Problema o Inconformidad: no se auditan regularmente ni se generan estadísticas sobre los logs referentes a la administración de red. Además no se hace ningún seguimiento de los logs en busca de cambios en las estadísticas o en las líneas de base.

Efectos: al no tener estas estadísticas no se calculan ni se grafican líneas de base y al no realizar monitoreos periódicos no se puede alertar al administrador sobre anomalías o posibles errores, en lo respectivo al tráfico de red o utilización de recursos del servidor. Además pueden generarse nuevos cuellos de botella en algún recurso del sistema, y el administrador puede no notarlo hasta que algún usuario se lo advierta.

Recomendación: el administrador o un encargado del área de Infraestructura del TIC's debería ser responsable de la monitorización de estos logs. Podrían generarse gráficos y estadísticas diarios o mensuales compuestos por datos suministrados por las distintas aplicaciones que se utilizan en la empresa y que generen logs.

Así podría obtenerse un reporte más detallado con datos y estadísticas como los siguientes:

- consumo de ancho de banda por terminal o por área de la institución o cuellos de botella en el tráfico de red,
- cantidad de tráfico genera cada aplicación utilizada por cada usuario
- cantidad de recursos que utilizan las aplicaciones.
- el estado de cada aplicación, (en cola, ejecutándose, esperando una respuesta, etc.),
- intentos de intrusión,
- estadísticas del uso de los protocolos

- páginas de Internet más visitadas, con información sobre los archivos descargados, los usuarios conectados, el horario, etc.

El seguimiento de estadísticas puede ser automatizado por medio de herramientas para Linux que realicen las tareas y sólo informen de las desviaciones con respecto a las líneas de base, a través de un mail o alerta.

Podrían generarse avisos cuando exista:

- incremento en el uso de Internet o del servicio de correo,
- tráfico excesivo de red, sectores o PC´s que superan el promedio de ancho de banda,
- incremento en los ataques o sospecha de intrusión,
- poco espacio en disco de servidores o de PC's,
- poca disponibilidad de CPU, memoria o algún recurso en los servidores,
- violaciones a las reglas de servicios de red, modificación en los permisos de los servicios o mala utilización de servicios.

Problema o Inconformidad: no se hicieron pruebas de auto-hackeo, escaneos o intentos de intrusión o de escucha en la red informática. Tampoco se hacen testeos periódicos de puertos o de los servicios que están habilitados.

Efectos: al no hacer pruebas o chequeos pueden pasar inadvertidas situaciones que solo serán reveladas utilizando casos prácticos.

Recomendación: sería conveniente programar chequeos periódicos de la red, incluyendo los siguientes controles:

- los servicios, su configuración y su buen funcionamiento;
- tratar de escuchar o hacer un ataque de intrusión periódicamente, para comprobar que la red sigue siendo inaccesible desde el exterior,
- realizar pruebas de auto-hackeo:
    - ✓ a los servidores, desde dentro del servidor,
    - ✓ a los servidores, desde la red interna,
    - ✓ a la intranet desde dentro de ella,
    - ✓ accesos desde el exterior y/o Internet.

Podrían utilizarse herramientas que permiten hacer estas inspecciones en la red en forma automática, para comprobar en qué estado está y determinar si existen vulnerabilidades en algunos sectores de acuerdo a líneas de base ingresadas por el administrador.

Además sería posible hacer auto-escaneos para verificar los recursos compartidos, y auto-hackeos para prevenir ataques de intrusión.
Sugerimos documentar las pruebas y sus resultados cada vez que se realicen.

7 - PLAN DE CONTINGENCIAS

7.1 PLAN DE ADMINISTRACIÓN DE INCIDENTES

No se hallaron debilidades significativas con respecto a este tema.

7.2 BACKUP DE EQUIPAMIENTO

Problema o Inconformidad: no se realizan pruebas periódicas de los mecanismos de respaldo de los servidores.
Efectos: ante una emergencia, puede ocurrir que estos mecanismos no funcionen correctamente o que los responsables de áreas del TIC's no desempeñen sus funciones correctamente por falta de práctica.
Recomendación: deberían realizarse planes de prueba periódicas, comprobando todos los mecanismos de respaldo con los que cuentan los servidores de la institución.

Problema o Inconformidad: los servidores de la institución se encuentran en la misma habitación física.
Efectos: ante un incidente, se puede utilizar un servidor en reemplazo del otro. Pero en el caso que la habitación donde se encuentran los servidores resulte afectada por una emergencia, todos los equipos quedarían inutilizados.
Recomendación: podría ser útil que alguno de los servidores, cuyas características son idénticas, se ubique en otra habitación o en otro edificio de la universidad. Esta situación puede resultar beneficiosa ante cualquier contingencia ocurrida en el departamento del TIC's.
Esta modificación no resultaría tan costosa ya que solo sería necesaria una habitación libre a la cual se le realizarían modificaciones mínimas de manera que funcione como cuarto de datos alternativo con las mismas condiciones de seguridad sugeridas para el CPD principal.
De esta manera, ante cualquier contingencia, por ejemplo si se produce una rotura del panel de control de energía independiente del departamento TIC's, el sistema

informático no se vería afectado, debido a que se contaría con un servidor alternativo en otro lugar físico, específicamente en otro edificio.

7.3 PLAN DE RECUPERACIÓN DE DESASTRES

7.3.1 ACCION PREVENTIVA

Problema o Inconformidad: no se asignan prioridades a los sistemas de información ni a los equipos de hardware de la red física.

Efectos: al no asignar niveles de prioridad a los sistemas o equipamientos no es posible determinar cuáles son los que deberían recuperarse de inmediato en caso de una emergencia.

Recomendación: se debería asignar un orden de importancia a cada uno de los sistemas de información y de los equipos de la red, de acuerdo al análisis de riesgo y al impacto que representaría para la universidad. La prioridad mayor la tendrá aquel sistema que es más importante a la hora de recuperar la operatividad luego de un desastre, los equipos deben estar señalizados o etiquetados de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.

Problema o Inconformidad: no se han identificado las funciones más críticas para las actividades del departamento del TIC's.

Efectos: al no identificar las funciones que interrumpen la productividad del departamento debido a su criticidad, se corre el riesgo de no tenerlas en cuenta en el momento de la restauración del sistema.

Recomendación: sería conveniente definir las funciones o servicios del departamento que sean más críticos. Cada jefe o encargado de área debe interactuar con el Director y definir estos servicios junto con los recursos mínimos necesarios para su funcionamiento, y asignarles una prioridad en el plan de restauración.

Además, sería conveniente identificar las contingencias que podrían ocurrir para cada nivel de servicio determinando, considerando:

- Cuáles serían los peores problemas a los que se puede ver sometido el departamento del TIC's, cuáles serian las peores contingencias
- Cuáles serían las más probables
- Cuáles son las que ocurren más a menudo
- Cuáles son las que no ocurren nunca

Problema o Inconformidad: no se hacen simulaciones de siniestros.

Efectos: sin estas simulaciones no será posible comprobar que los empleados hayan comprendido las tareas a su cargo y será imposible predecir su comportamiento ante una emergencia.

Recomendación: para el entrenamiento del personal deberían generarse simulacros de siniestros y así evaluar la efectividad del plan.

7.3.2 PLAN DE ACCIÓN

Problema o Inconformidad: en el departamento del TIC's no hay planes formales para la administración de incidentes ni funciones claras que deba realizar el personal durante una contingencia, ya que no hay responsabilidades asignadas.

Efectos: al no haberse designado claramente las responsabilidades de los empleados frente a una emergencia, las acciones que se tomen en caso de contingencia resultarán caóticas, comprometiendo la integridad de los datos y equipos.

Recomendación: debería conformarse un plan de emergencias, determinando los procedimientos a llevar a cabo para cada contingencia identificada en la estrategia proactiva. Estas tareas deberían estar claramente definidas y documentadas, y tener asignado un responsable para su ejecución, considerando los distintos escenarios posibles (por ejemplo durante el día o la noche).

Ejemplos de las tareas a desarrollar pueden ser:

- En caso de incendio:
  - ✓ Identificar las vías de salida.
  - ✓ Generar un plan de evacuación del personal.
  - ✓ Desarrollar un plan de puesta a buen recaudo de los activos.
  - ✓ Ubicación y señalización de los elementos contra el siniestro.
- En caso de intrusión interna o externa:
  - ✓ Desconectar los servidores.
  - ✓ Cerrar todos los accesos a los datos.
  - ✓ Rastrear al intruso.

Deberían contemplarse las siguientes características:

- Debería estar documentado y testeado antes de su puesta en práctica.
- Debería basarse en un análisis de riesgo, determinando que acciones merecen estar incluidas.

- Debería abarcar todo el edificio, no solo el departamento del TIC's.
- Debería entrenarse a los responsables y a los usuarios.
- Debería mantenerse actualizado de acuerdo a nuevos puestos de trabajos y funciones.
- Debería ser retroalimentado después de cada incidente.
- Debería ser probado frecuentemente.
- Debería contener la siguiente información:
    - ✓ Objetivo del plan.
    - ✓ Modo de ejecución.
    - ✓ Tiempo de duración.
    - ✓ Costos estimados.
    - ✓ Recursos necesarios.
    - ✓ Evento a partir del cual se pondrá en marcha el plan.

7.3.3 PLAN REACTIVA

Problema o Inconformidad: no se documentan los acontecimientos ocurridos durante las emergencias, ni se hacen evaluaciones formales de los daños sufridos.

Efectos: al no documentarse los acontecimientos ni daños acontecidos, se corre el riesgo de no hacer las correcciones necesarias para que no ocurran las mismas contingencias. Puede ocurrir también que durante el incidente se realicen modificaciones de urgencia en alguna parte del sistema y éstas no queden documentadas.

Recomendación: sugerimos que se documente la realización de las siguientes actividades después de que ha ocurrido algún desastre:

- Determinar la causa del daño.
- Evaluar la magnitud del daño que se ha producido.
- Que sistemas se han afectado.
- Qué modificaciones de emergencia se han realizado.
- Que equipos han quedado no operativos,
- Cuales se pueden recuperar y en cuanto tiempo.

Se debería actualizar la documentación del TIC's con las modificaciones implementadas y las acciones correctivas que se llevaron a cabo como consecuencia del incidente.

Problema o Inconformidad: Una vez ocurrido el siniestro, el administrador o encargado por el director del TIC's, realiza las actividades de recuperación sin respaldarse en un plan o manual formal de procedimientos.
Efectos: al no tener una guía es muy probable que se cometan errores u omisiones en las acciones de restablecimiento.
Recomendación: se debería asignar el papel de coordinador a un empleado, que se encargará de las operaciones necesarias para que los sistemas funcione correctamente después de la emergencia. Ésta persona debería determinar las acciones a seguir de acuerdo al tipo de emergencia que ha ocurrido, basándose en el plan de emergencias. Un ejemplo de acciones principales a seguir en el caso de la caída de los sistemas serían:

- Setup e instalación de los componentes de hardware necesarios.
- Carga del software del sistema.
- Instalación del software de aplicación.
- Provisión de los datos necesarios (backup), incluyendo archivos de configuración.
- Re-arrancar el equipo.
- Se debe asegurar que se empiece a auditar una vez que se reinicia.

Problema o Inconformidad: debido a que no hay implementado un plan de acción en caso de desastres, no se realiza una retroalimentación con los datos obtenidos luego de una emergencia.
Efectos: si no se aprende del resultado de estas acciones, no será posible evitar la misma contingencia en el futuro ni mejorar la eficacia de las directivas.
Recomendación: se debería tener en cuenta la experiencia que se obtiene luego de una contingencia para retroalimentar el plan, y así obtener uno de mayor eficiencia. Esto se logra generando una lista de recomendaciones para minimizar los riesgos de futuros incidentes similares. En base a la experiencia obtenida, evaluar:

- El desempeño del personal inmerso en la emergencia, y reordenar la lista.
- Si algún elemento o tarea tenía asignada una prioridad que no le correspondía, se deberían modificar estas prioridades.
- La introducción de actividades que no se contemplaron en el plan de emergencia.
- La generación de sugerencias y posibles mejoras.

Atento a las debilidades mencionadas anteriormente, el departamento de Tecnología debe analizar la situación planteada a los efectos de determinar si corresponde la iniciación de acciones pertinentes.

5.10 IMPACTO DE LA PROPUESTA

La propuesta ejecutada persigue mejorar el desarrollo del departamento del TIC's en las diferentes servicios que ofrece a la comunidad universitaria, donde se puede agilitar procesos que disminuyan costos, el impacto para los que forman parte del departamento del TIC's es significativo y beneficioso ya que les permite ir mejorando en sus actividades y con esto conlleva a la satisfacción y confiabilidad del resto de los empleados de la UNEMI que utilizan los sistemas informáticos y así cada vez a mas los estudiantes pueden utilizar los servicios de ofrece el TIC's para su formación académica, lo que lleva a aportar sin duda al proceso de acreditación que persigue la UNEMI.

5.10.1 ANÁLISIS DEL IMPACTO SOCIAL

Con el mejoramiento de los servicios que ofrece al TIC's se fomenta el uso de las servicios tecnológicos a los estudiantes y docentes en las prácticas académicas, favoreciendo el desarrollo académico y profesional de los alumnos, y poder conseguir de esta manera la eficiencia terminal con las destrezas necesarias para asumir el reto del mercado laboral. Así se va ir contribuyendo entonces como se menciono anteriormente a la formación integral de los estudiantes y la búsqueda de la excelencia académica que es una de los objetivos de la UNEMI.

5.10.2 ANÁLISIS DEL IMPACTO AMBIENTAL

Con la propuesta de una auditoria de seguridad informática en el TIC's no representa un impacto ambiental significativo ya que se desarrolla haciendo uso de la infraestructura y los equipos existentes en el departamento.

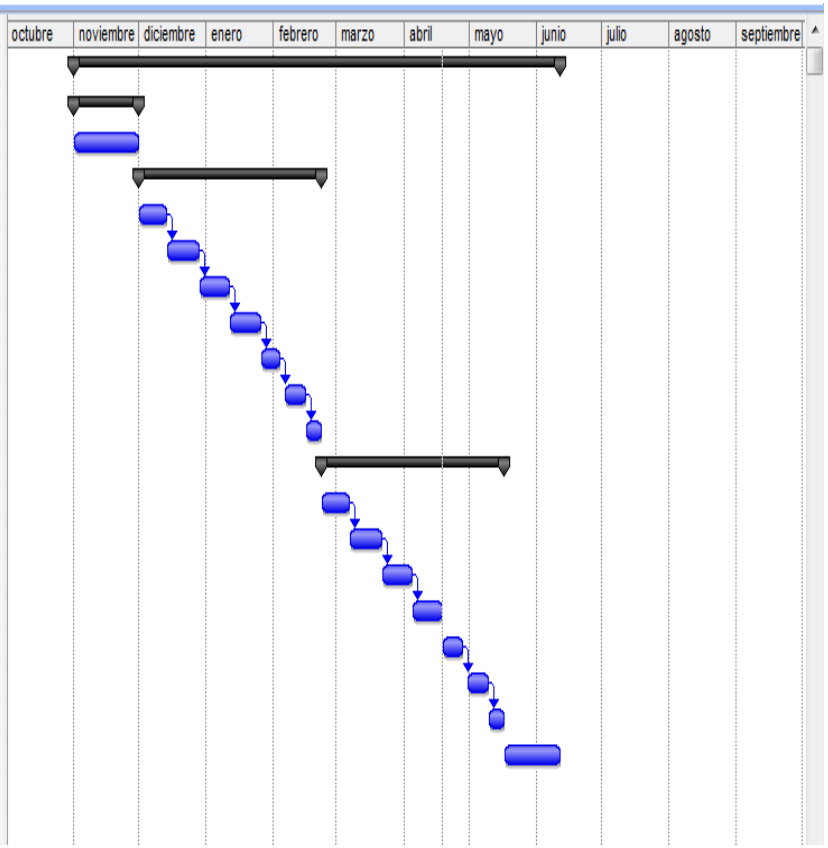
Además se puede indicar que la UNEMI cuenta con un área de ensamblaje y reciclaje en la Unidad Académica Ciencias de la Ingeniería el cual está encargado de reutilizar o reciclar los equipos informáticos que ya cumplieron su ciclo de vida útil a base de los informes técnicos que realiza el departamento del TIC's.

De igual forma en la universidad se está ejecutando un proyecto de reciclaje de papel y plástico, estos proyectos son un aporte significativo para reducir la contaminación. Además el uso de la tecnología se ha convertido hace muchos años en un recurso primordial para la ejecución de las actividades, lo que implica mayor consumo de energía eléctrica, pero actualmente los equipos informáticos y tecnológicos tienen características que ayudan al cuidado del medio ambiente, y reducción de consumo como: energía eléctrica, reutilización de piezas y partes de los equipos informáticos y reducir el consumo de papel (correo electrónico y Fax ip).

5.11 Cronograma de la implementación de la propuesta

Diagrama de Gantt

	Nombre de tarea	Duración	Comienzo	Fin
1	**Analisis de la Auditoria de Seguridad Informatica**	**160 días?**	**mar 01/11/11**	**lun 11/06/12**
2	**Informe de recoleccion de Informacion**	**22 días?**	**mar 01/11/11**	**mié 30/11/11**
3	Recoleccion de Informacion y Analisis	22 días?	mar 01/11/11	mié 30/11/11
4	**Evaluacion de la Seguridad Informacion**	**60 días?**	**jue 01/12/11**	**mié 22/02/12**
5	Seguridad Logica	9 días?	jue 01/12/11	mar 13/12/11
6	Seguridad en las Comunicaciones	11 días?	mié 14/12/11	mié 28/12/11
7	Seguridad de las Aplicaciones	10 días?	jue 29/12/11	mié 11/01/12
8	Seguridad Fisica	10 días?	jue 12/01/12	mié 25/01/12
9	Evaluacion de la Administracion de CPD	7 días?	jue 26/01/12	vie 03/02/12
10	Evaluacion de la Auditoria y Revisiones	8 días?	lun 06/02/12	mié 15/02/12
11	Evaluacion Plan de Contingencias	5 días?	jue 16/02/12	mié 22/02/12
12	**Recomendaciones de la Seguridad Informacion**	**60 días?**	**jue 23/02/12**	**mié 16/05/12**
13	Seguridad Logica	9 días?	jue 23/02/12	mar 06/03/12
14	Seguridad en las Comunicaciones	11 días?	mié 07/03/12	mié 21/03/12
15	Seguridad de las Aplicaciones	10 días	jue 22/03/12	mié 04/04/12
16	Seguridad Fisica	10 días	jue 05/04/12	mié 18/04/12
17	Evaluacion de la Administracion de CPD	7 días	jue 19/04/12	vie 27/04/12
18	Evaluacion de la Auditoria y Revisiones	8 días	lun 30/04/12	mié 09/05/12
19	Evaluacion Plan de Contingencias	5 días	jue 10/05/12	mié 16/05/12
20	Conclusiones y recomendaciones	18 días	jue 17/05/12	lun 11/06/12



5.12 Lineamiento para evaluar la propuesta

Para la evaluación de la propuesta se considera:

- Interés de las autoridades y empleados universitarios para la realización del proyecto, que es considerado como un objetivo apoyar el desarrollo de las TIC.
- Estadísticas semestral del nivel de la satisfacción y confiabilidad de uso de los servicios informáticos que brinda el departamento del TIC's a la comunidad universitaria.
- Porcentaje estadístico de participación o utilización de los sistemas informáticos que ofrece el TIC's a la comunidad universitaria.
- Porcentaje del crecimiento tecnológico del TIC's.

Conclusión.

El trabajo de auditoría realizada se concluye indicando que el estado de la seguridad de la información en el departamento del TIC's se puede denominarse como: Favorable con Salvedades.
Considerando los elementos de juicio obtenidos durante las tareas efectuadas, se ha determinado que si bien existen prácticas tendientes a garantizar un adecuado nivel de seguridad del sistema informático y de comunicaciones, las mismas no son suficientes ni se encuentran ordenadas en un reglamento o normativa.

El departamento del TIC´s, se beneficia de las recomendaciones, dadas para el mejoramiento de los servicios informáticos precautelando su información.
Entre los beneficios que consideran de mayor importancia tenemos:

1. Incrementar la confiabilidad de los usuarios.
2. Mejorar el servicio de red y comunicaciones
3. Mejora en soporte usuarios.
4. Protección de los datos.
5. Mejora de la administración de los servicios informáticos.

Recomendación.

Luego de la realización de la auditoria Informática se debe llevar a cabo las recomendaciones expuestas:

- Reducir el ambiente de riesgo vigente.
- Disponer de las medidas de control interno necesarias.
- Disminuir el grado de exposición de los sistemas que se procesan.
- Incrementar la confiabilidad, integridad y disponibilidad de la información.
- Revisiones periódicas de cumplimento de políticas de seguridad informática.
- Y optimizar los procesos orientados al cumplimiento de los objetivos del departamento y de la universidad.

Bibliografía

MAGLIONA MARKOVICTH Claudio Paúl, LÓPEZ MEDEL Macarena, Delincuencia y Fraude Informático, Editorial Jurídica de Chile. 1999.

MANZANARES, José Luis y CREMADES, Javier. "Comentarios al Código Penal"; La Ley- Actualidad, Las Rozas (Madrid), 1996.

MERLAT, Máximo, Seguridad Informática: Los Hackers, Buenos Aires Argentina, 1999, Publicación hecha en Internet. www.monografías.com

[1] A. Reyes Ponce, "Planificación Estratégica", www.itescam.edu.mx/principal/sylabus/fpdb/recursos/r69371.DOCX, http://www.monografias.com/trabajos37/planeacion/planeacion.shtml

[2] J. A. Fernández Arenas, "La Administración", 2009, http://misapuntesanayeli.blogspot.com/2009/04/concepto-e-importancia-de-la-planeacion.html, http://html.rincondelvago.com/administracion-mexicana.html

[3] Guzmán, "Organización", http://sistemas.itlp.edu.mx/tutoriales/procesoadmvo/tema3_1.htm, http://www.wikilearning.com/monografia/las_organizaciones_y_su_evolucion-concepto_de_organizar/11631-1

[4] Burt K. Scanlan, "Otros Conceptos de Administración", 2006, http://www.monografias.com/trabajos17/procesos-administrativos/procesos-administrativos.shtml, http://www.gestiopolis.com/canales7/mkt/administracion-direccion-y-liderazgo.htm

[5] Lerner y Baker, "Definición de Dirección", http://sistemas.itlp.edu.mx/tutoriales/procesoadmvo/tema5_1.htm, http://www.gestiopolis.com/canales7/mkt/administracion-direccion-y-liderazgo.htm

[6] T. Gillis, "Riesgos Informáticos", 2007, http://www.riesgosinformaticos.com.ar/2007/11/04/mejores-practicas-para-evitar-la-perdida-de-informacion/, http://seguridad-informacion.blogspot.com/2007/10/mejores-prcticas-para-evitar-la-prdida.html.

[7] Bradley R. Hunter, http://www.dienerlaw.net/hunter.html

[8] Cordeiro, "Medios de Comunicación y su relación con las Tecnología de Información", 1998, http://advenimiento7.blogspot.com/2006/12/medios-de-comunicacion-y-su-relacion.html

Material Complementario:

http://es.wikipedia.org

http://www.monografias.com

http://www.slideshare.net/Decimo/arquitectura-3-capas

"SET Software Compliance Testing". SET Secure Electronic Transaction LLC. www.setco.org

"Seguridad en Internet". Microsoft. www.microsoft.com

ANEXO 1

Encuesta realizada al personal de la UNEMI que maneja los sistemas informáticos o que tiene relación directa con los servicios (Sistemas Informáticos, correo electrónico, telefonía IP e Internet) que presta el departamento del TIC´s.

Marque con una X su respuesta.

Pregunta 1

¿Conoce usted que es una Auditoria de Sistemas de Información?

SI		NO	

Pregunta 2

¿Qué sistemas informáticos, utiliza comúnmente para realizar sus labores de trabajo?

WORD	
EXCEL	
Sist. Académicos	
Sist. Administrativos	
PROJECT	
POWER POINT	
OUTLOOK	
OTROS	

Pregunta 3

¿Cómo considera usted los servicios informáticos que presta el departamento del TIC's (sistemas, internet, correo, pagina web)?

MUY BUENO	
BUENO	
REGULAR	
MALO	

Pregunta 4

¿Las capacitaciones y soportes técnicos recibidos de parte del Dpto. del TIC's como usted lo considera?

MUY BUENO	
BUENO	
REGULAR	
MALO	

Pregunta 5

¿Conoce usted cuál es su función del departamento de Auditoría Interna de la UNEMI?

SI CONOCE	
NO CONOCE	
NO ESPECIFICA	

Pregunta 6

Conoce usted si en el Departamento de Tecnología tiene algún sistema seguridad para ingresar a sus instalaciones?

SI		NO	

Pregunta 7

Qué grado de importancia tiene los sistemas informáticos desarrollados por la UNEMI como herramienta de trabajo?

MUY IMPORTANTE	
IMPORTANTE	
MEDIANAMENTE IMPORTANTE	
NADA IMPORTANTE	

Pregunta 8

¿La información almacenada y consultada por medio de los sistemas informáticos es confiable para usted?

SI		NO	

Pregunta 9

¿Qué grado de importancia daría usted, si le consultan que se va auditar al departamento del TIC's?

MUY IMPORTANTE	
IMPORTANTE	
MEDIANAMENTE IMPORTANTE	
NADA IMPORTANTE	