INSTITUTO SUPERIOR TECNOLÓGICO BOLIVARIANO

DE TECNOLOGÌA

PROYECTO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN ANALISIS DE SISTEMAS

TEMA:

MEJORAMIENTO DEL PLAN DE CONTINGENCIA EN EL AREA DE TICS DEL INSTITUTO SUPERIOR TECNOLÓGICO BOLIVARIANO DE TECNOLOGÍA

Autor:

Michael Mora Vanegas

Tutor:

Lcdo. Iván Darwin Tutillo Arcentales

Guayaquil, Ecuador

2015

CERTIFICACIÓN DE LA ACEPTACIÓN DE TUTORIA

En mi calidad de Tutor del Proyecto de Investigación, nombrado por el Consejo Directivo del Instituto Superior Tecnológico Bolivariano de Tecnología.

CERTIFICO:

Que he analizado el proyecto de investigación con el tema: **"Mejoramiento del Plan de contingencia en el área de tics del Instituto Superior Tecnológico Bolivariano de Tecnología",** presentado como requisito previo a la aprobación y desarrollo de la investigación para optar por el título de:

TECNÓLOGO EN ANÁLISIS DE SISTEMAS

El problema de investigación se refiere a: **¿Qué incidencia tiene la suficiencia de los planes de contingencia del área de Tics en el desempeño de los actores en el Instituto Superior Tecnológico Bolivariano de Tecnología?**

El mismo que considero debe ser aceptado por reunir los requisitos legales y por la importancia del tema:

Presentado por el Egresado: **Michael Alexander Mora Vanegas**

Tutor: **Lcdo. Iván Darwin Tutillo Arcentales**

AUTORÍA NOTARIADA

Los criterios e ideas expuestos en el presente trabajo de graduación con el tema: **"Mejoramiento del Plan de contingencia en el área de tics del Instituto Superior Tecnológico Bolivariano de Tecnología",** de la carrera Análisis de Sistemas del Instituto Superior Tecnológico Bolivariano de Tecnología, son de absoluta responsabilidad del autor y no constituye copia o plagio de otra tesis presentada con anterioridad.

DEDICATORIA

Dedico esta tesis a todos aquellos que creyeron en mí, a aquellos que me acompañaron en cada paso que daba hacia la culminación de mis estudios, a aquellos que esperaban que lograra terminar la carrera, a todos aquellos que aposaban a que lo lograría, a todos ellos les dedico esta tesis

Sr. Michael Mora Vanegas

AGRADECIMIENTO

A mi director de tesis, Isi. Iván Tutillo por su esfuerzo y dedicación, quien con sus conocimientos, su experiencia, su paciencia y su motivación ha logrado en mí que pueda terminar mis estudios con éxito.

También me gustaría agradecer a mis profesores durante toda mi carrera profesional porque todos han aportado con un granito de arena a mi formación, y en especial a mi familia por ampollarme tanto.

Son muchas las personas que han formado parte de mi vida profesional a las que les encantaría agradecerles su amistad, consejos, apoyo, ánimo y compañía en los momentos más difíciles de mi vida. Algunas están aquí conmigo y otras en mis recuerdos y en mi corazón, sin importar en donde estén quiero darles las gracias por formar parte de mí, por todo lo que me han brindado y por todas sus bendiciones.

Sr. Michael Mora Vanegas

TECNOLOGÍA EN ANALISIS DE SISTEMAS

Proyecto previo a la obtención del título: Tecnólogo en Análisis de Sistemas.

Tema

MEJORAMIENTO DEL PLAN DE CONTINGENCIA EN EL ÁREA DE TICS DEL INSTITUTO TECNOLÒGICO BOLIVARIANO

Autor: Michael Mora Vanegas .
Tutor: Lsi. Iván Tutillo Arcentales

RESUMEN

El presente trabajo de investigación se desarrolla observando las tareas diarias del departamento de Tics del Instituto Superior Tecnológico Bolivariano de Tecnología ITB, con la premisa de diseñar un plan de contingencia, que tenga suficiencia en su calidad. De las tareas diarias se evalúan la que tienen mayor número de requerimientos, por lo que deben ser atendidas aún bajo situación de emergencia para que los usuarios puedan seguir operativos. Son muchas las tareas en las que interviene el departamento de Tics, pero de esas sólo unas cuantas son las que ocurren con bastante regularidad, por lo que este trabajo va enfocado hacia el esfuerzo de tener los planes de contingencia que abarquen las tareas que con mayor regularidad ocurren y que representan algo más del 50% de las actividades que las áreas de este departamento atiende, donde la mayoría atiende el personal del área técnica. El área de tics es nueva y en su creación, por lo que deben renovarse estos planes. Se pudo observar unas actividades que no tenían planes por lo que también tendrán que crearse unos nuevos. Un diagnostico preliminar determina los planes que necesitan renovarse y/o crearse. Se toman las mejores prácticas en cada caso para proponer la mejora en el plan de contingencia que se sugiere y se socializa estos planes con el departamento de tics para su evaluación de factibilidad.

PALABRAS CLAVE:	CONTINGENCIA ITB TICS TECNICA ACADEMICA

TECNOLOGÍA EN ANALISIS DE SISTEMAS

Proyecto previo a la obtención del título: Tecnólogo en Análisis de Sistemas.

Tema

EVALUACIÓN Y MEJORAMIENTO DEL PLAN DE CONTINGENCIA EN EL ÁREA DE TICS DEL INSTITUTO TECNOLÒGICO BOLIVARIANO

Autor: Michael Mora Vanegas .
Tutor: Lsi. Iván Tutillo Arcentales

ABSTRACT

This research is developed observing the daily tasks of the Bolivarian tics department Technological Institute of Technology ITB, with the premise of designing a contingency plan that takes sufficiency in quality. Daily tasks are evaluated with the highest number of requirements, which must be met even under emergency so that users can continue operating. There are many tasks involved in tics department, but of those only a few are those that occur quite regularly, so this work is focused on the effort to have contingency plans covering more tasks regularly occur and represent more than 50% of the activities that this department serves areas, where most staff attending technical area. Tics area is new and in its creation, so these plans must be renewed. It was observed that some activities had no plans so you'll have to create new ones. A preliminary diagnosis determines the plans need to be renewed and / or created. Best practices are taken in each case to propose improvements in the contingency plan is suggested and these plans are socialized tics department for evaluation of feasibility

KEYWORDS: | CONTINGENCY ITB TICS TECHNICAL ACADEMIC

ÍNDICE DE CONTENIDO

CAPITULO I

1. EL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

1.1.1 UBICACIÓN DEL PROBLEMA EN UN CONTEXTO

El presente trabajo de investigación pretende describir los planes de contingencia utilizados dentro del plan general del área de Tic's del Instituto Superior Tecnológico Bolivariano de Tecnología, para luego realizar una evaluación de la suficiencia de estos planes dentro del marco de trabajo del año 2015. Las consideraciones generales para esta evaluación están bajo la óptica del criterio de una auditoria informática.

Una de las áreas más requeridas, debido a su respuesta a problemas informáticos, es el área de soporte técnico de las tic's por el hecho de estar a cargo de brindar soluciones de corta a largo plazo con el fin de resolver la incidencia que se llegue a presentar actualmente; como parte de las funciones que atañen a la tic's se encuentra la de brindar soporte técnico a dispositivos, gestionar el alta y baja de usuarios para los diferentes sistemas, correo electrónico, gestionar la instalación de puestos de trabajo, de red y de telefonía, brindar soporte tecnológico a eventos, asesorar y velar por la seguridad informática, entre otros, en el ámbito de rectorado, de las aulas en las que se imparten las clases, en las oficinas y los laboratorios con el fin de

mantener el funcionamiento óptimo de los mismos y prevenir el retraso con las actividades de los usuarios del tecnológico.

Las aulas de informática son punto de encuentro y de paso de prácticamente todo el alumnado y profesorado de un centro educativo, por lo que de nada sirve disponer de un buen equipamiento, moderno y potente, si éste no ofrece la funcionalidad necesaria para un buen desarrollo de las clases, que cubran las expectativas tanto de los profesores, con los equipo en clase, como de los alumnos con los equipos en laboratorio y cyber. La funcionalidad de las aulas de informática, es para que los profesores puedan impartir sus clases en condiciones óptimas y que el cumplimiento de su programación sea del 100%, así el alumno podrá aprovechar al máximo el tiempo y el esfuerzo de su docente.

Es necesario, por tanto, para el desarrollo de la tarea docente disponer de aulas de informática en los centros que ofrezcan garantías respecto a su funcionalidad, estado de los recursos y seguridad en el uso de los mismos. Disponer de una estructura de aula acorde a las necesidades reales del docente es tarea de la administración de los bienes informáticos en las aulas de clase como en las oficinas del Instituto Superior Tecnológico Bolivariano de tecnología, cuya responsabilidad debe ir más allá de enviar material informático a los centros, es decir, proveer los medios software necesarios para su buen uso, mantenimiento y actualización.

El alcance con que se lleve a cabo la planificación varía según el tamaño y la complejidad de la entidad, el conocimiento del tipo de actividad en que el ente se desenvuelve, de la calidad de la organización y del control interno de la entidad en vista del acelerado cambio en la industria de las tecnologías de la información y la comunicación, las empresas deben orientarse a mejorar de forma continua sus procesos, aplicando nuevas metodologías y conceptos que

las lleven a mejorar su espectro de competitividad permitiéndole mantenerse sobre un entorno globalizado.

1.1.2 SITUACIÓN CONFLICTO

El área de Tic's se ve involucrada en las actividades de todas las demás áreas del tecnológico, siendo vista como un área que presta servicios internos para que el operativo continúe su trabajo rutinario.

Diariamente se presentan actividades y situaciones imprevistas que deben ser resueltas por el área de Tic's, pero que por su cantidad no pueden ser cubiertas en forma inmediata por el escaso personal técnico, provocando que existan retrasos en las áreas afectadas y creando un conflicto en aquellos que no pueden ser atendidos con la celeridad que requieren.

Las actividades y situaciones imprevistas más frecuentes que resuelve el departamento de Tics se describen a continuación.

1.1.2.1. IMPLEMENTACIÓN DE PARCHES EN APLICACIONES WEB.

Aunque son ya muchas las compañías que se han puesto 'serias' en cuando a la implementación de parches y actualizaciones de las aplicaciones, esta práctica no cubre el perfil entero de la seguridad de aplicaciones.

La topología actual de aplicaciones empresariales es mixta y está compuesta tanto por programas internos como externos. Muchos de estos programas no son más que pequeños scripts PHP o AJAX. Y estos son precisamente los que más riesgo conllevan porque son sencillos y fáciles de descifrar.

Las compañías deben tener a mano un listado de todas las aplicaciones Web y scripts que residen en la red. Asegúrese de que dispone de las últimas versiones de las aplicaciones y componentes que hay detrás de los wikis y blogs, por ejemplo. En el caso de aplicaciones custodiadas, mantenga un fichero de los scripts que éstas puedan incorporar.

Esto significa la monitorización periódica de servicios de seguridad como CERT y las páginas Web o comunidades que ofrecen estos servicios. Asegurar la integridad de las aplicaciones que son un punto de entrada a la red corporativa es una inversión sin precio.

Esta actividad la realiza un técnico de programación especialista en PHP, AJAX y PHYTON, su trabajo lo desarrolla en el servidor web.

Situación inicial: No aplica, debido a que inicialmente no había programación web desarrollada, a raíz de la compra del SGA y la contratación de programadores se da inicio a esta actividad.

1.1.2.2. HABILITACIÓN DEL ACCESO REMOTO SEGURO

Una fuerza laboral con una movilidad cada vez mayor, el uso de múltiples dispositivos y el traslado de las aplicaciones a la nube están desdibujando los límites del perímetro tradicional de seguridad de redes. Las empresas deben resolver los problemas de seguridad del acceso remoto, incluso cuando los empleados se encuentran en la oficina.

Cuando los recursos corporativos se encuentran dispersos entre bases de datos y aplicaciones locales, basadas en la nube y basadas en la web, la necesidad de políticas unificadas de autenticación se vuelve crítica para garantizar la transparencia y consistencia de los controles de acceso.

Esta operación se la realiza en la consola de los servidores de aplicaciones que están ubicadas en el departamento de sistemas.

1.1.2.3. MONITOREO Y GESTIÓN DE LA SEGURIDAD

El monitoreo se realiza en el área de tics y la persona a cargo es el jefe de mantenimiento, el cual lleva una bitácora de control.

Para esta tarea es necesaria la implementación de sistemas y procesos para la gestión de los eventos de seguridad en el ambiente tecnológico, haciendo posible un control mayor del ambiente de trabajo.

El encargado de esta tarea es el jefa de del área de tics y se realiza en el cuarto de administración donde se encuentran físicamente la pantalla que muestra las actividades de las cámaras.

1.1.2.4. ATENCIÓN A LOS DESARROLLOS DE PROGRAMAS

Esto se hace a partir de los usuarios particularmente involucrados, para determinar los requerimientos de información dentro de una organización pueden utilizarse diversos instrumentos, los cuales incluyen: muestreo, el estudio de los datos y formas usadas para la organización, la entrevista, los cuestionarios; la observación de la conducta de quien tomo la decisiones, así como de su ambiente. Se hace todo lo posible por identificar qué información requiere el usuario para desempeñar sus tareas.

Esta tarea es realizada por los programadores del área de tics, donde cada uno de ellos está a cargo de uno o máximo dos modulo del sistema y tienen una coordinación y supervisión de sus tareas, la cual está liderada por la gerente de sistemas.

1.1.2.5. REINICIAR SERVIDORES

Reiniciar un servidor en un centro de datos conlleva más que pulsar el botón de encendido. Dado que las políticas de seguridad de los centros de datos suelen ser complicadas, es necesario disponer de una solución adecuada para poder realizar el mantenimiento más urgente cuando no podemos acceder fácilmente o con rapidez al centro de datos. Y es aquí donde entra el sistema de reinicio remoto.

El encargado de esta tarea es el jefe de mantenimiento del área de tics y se realiza en el cuarto del rack donde se encuentran físicamente los servidores de datos, de aplicaciones y de internet.

1.1.2.6. REVISIÓN DE EQUIPOS EN AULA

Para poder realizar esta tarea es necesario un control periódico a las aulas del campus para poder identificar posibles problemas en el mismo dependiendo de la magnitud del daño se toma medidas en la reparación los encargados de esta tarea son los encargados del área de tics.

Esta tarea es realizada por auxiliares de mantenimiento, los que en ocasiones son practicantes de la carrera de Tecnología en Análisis de Sistemas y lo realizan en cada aula de cualquiera de las cuatro sedes

1.1.2.7. INSTALACIÓN DE PROGRAMAS

La instalación de los programas computacionales (software) es el proceso fundamental por el cual los nuevos programas son transferidos a un computador con el fin de ser configurados, y preparados para ser ejecutados en el sistema informático, para cumplir la función por la cual fueron desarrollados, funciones como la del aula y laboratorio de clase, equipo del docente en su sala, equipo de trabajo del personal administrativo.

Los encargados de esta tarea son el personal de mantenimiento del área de tics y lo hacen en el sitio donde están los equipos que requieren esta atención, esto es cualquiera de las cuatro sedes del tecnológico.

1.1.3. DELIMITACIÓN DEL PROBLEMA

Campo: Tecnología de información
Área: Auditoria de sistemas
Aspecto: Evaluación de plan de contingencia
Periodo: 2015

1.1.4. PLANTEAMIENTO O FORMULACIÓN DEL PROBLEMA

¿Qué incidencia tiene la suficiencia de los planes de contingencia del área de Tics en el desempeño de los actores en el Instituto Superior Tecnológico Bolivariano de Tecnología?

1.2. VARIABLES DE LA INVESTIGACIÓN

VARIABLE INDEPENDIENTE:

Actividades del área de Tics

VARIABLE DEPENDIENTE

Planes de contingencia.

1.3. OBJETIVOS DE LA INVESTIGACIÓN

1.3.2. OBJETIVO GENERAL

Encontrar posibles mejoras que contribuyan a elevar el rendimiento del desempeño del área de tics en la atención a los problemas de usuario y propios del departamento, a través de una auditoria a la suficiencia de los planes de contingencia del área de Tic's del Instituto Superior Tecnológico Bolivariano de Tecnología.

1.3.3. OBJETIVOS ESPECÍFICOS

- Diagnosticar el estado actual del departamento de Tics en relación a las actividades de atención a los problemas de usuario.
- Fundamentar los aspectos teóricos de los planes de contingencia.
- Sugerir un plan de mejoras para los planes de contingencia del departamento de Tic's

1.4. JUSTIFICACIÓN E IMPORTANCIA

Realizar un Plan de evaluación para la implementación de políticas operativas e inclusión tecnológica, permitirán mejorar el flujo de atención y comunicación entre el departamento de tics y los demás departamentos de la institución

Como se puede colegir, en lo visto en la definición del problema, que son varios los riesgos informáticos a los que se enfrenta una empresa y que se ven acrecentados por el uso de internet. Por lo cual, resulta pertinente realizar una evaluación sobre los respectivos mecanismos que ayuden a reducir estos riesgos, lo que evitaría pérdidas económicas considerables mediante la implementación de las recomendación de esta investigación.

Las recomendaciones de esta investigación buscan lograr un mejor rendimiento del esfuerzo del personal de Tics al momento de atender algún imprevisto bajo la óptica de los planes de contingencia aprobados.

Desde el punto de vista académico el desarrollo del proyecto puede tener un gran impacto porque permite obtener conocimientos específicos de cómo realizar una evaluación que permita al Instituto Tecnológico Bolivariano de Tecnología hacer frente a algún inconveniente informático, visualizando los planes de contingencia planteados para ello. Por lo que es necesario evaluar los procesos que realiza el área de Tic's y en base a esos resultados poder implementar procesos de contingencia viables como resultado de esta investigación

En el ámbito social y económico se genera un gran beneficio al Tecnológico ya que se evaluará los procesos de contingencia en su viabilidad y seguridad en ser implementados, mejorando la respuesta ante cualquier eventualidad y por ende garantizando la continuidad del negocio y evitando pérdidas económicas.

También, el garantizar la continuidad del negocio se previenen y se mejora la atención a problemas que pudieran detener el buen funcionamiento en el áreas de Tics a través de la implantación de un sistema de gestión de seguridad que realicen continuamente la evaluación a la suficiencia de los planes de contingencia del Instituto Superior Tecnológico Bolivariano de Tecnología, y

así conseguir un impacto positivo en los clientes internos (estudiantes y docentes).

Gracias a la investigación que hemos realizado en este capítulo, se evidencia el problema que se quiere atender en la administración y organización de actividades en el área de Tics, por eso hacemos la propuesta de Evaluar su plan de contingencia mejorar estos procesos y para que los usuarios mejoren su desenvolvimiento en el ámbito laboral.

CAPITULO II

MARCO TEORICO

2.1. FUNDAMENTACIÓN TEÓRICA

La metodología y la mecánica operativa utilizada para realizar la investigación basada en observaciones, entrevistas y encuestas aplicadas a los involucrados en el departamento de tics del Instituto tecnológico Bolivariano con el fin de evaluar la suficiencia del plan de contingencia del área de Tics.

2.1.1. ANTECEDENTES HISTORICOS

Creación del área de tics

El área de tics del Instituto Superior Tecnológico Bolivariano de Tecnología fue formalmente creado en junio del 2012, anteriormente se tenía una jefatura de sistemas que proponía soluciones de programación y las implementaba en todo el tecnológico, esta jefatura no se involucraba con la atención a los requerimientos tecnológicos los cuales eran solucionados directamente por el señor Rector el cual tiene formación de Licenciado en Sistemas de Información; sin embargo y debido al inusual incremento de estudiantes y por ende del aumento de los servicios sistematizados, hubo que recurrir a la implementación de un área de tics que resuelva dicha sistematización.

2.1.2. PRIMEROS PLANES DE CONTINGENCIA

Una vez creada el área de tics, se establecieron sus responsabilidades y se diseñaron los primeros planes de contingencia para hacer frente a posibles eventos negativos y a los requerimientos por servicio diario, esto ocurrió en octubre del año 2012. Los planes de contingencia que se diseñaron, consideraron la infraestructura y necesidades conocidas a esa fecha, principalmente se buscaba una aplicación web para el sistema académico ya que el desarrollado hasta ese momento estaba quedando poco práctico.

2.1.3. IMPLEMENTACIÓN DE LOS SERVIDORES WEB

La búsqueda de soluciones para el sistema académico, logro encontrar un software web que requería de la Implementación de servidores web y de servicios de internet en todo el edificio matriz, la planificación de soluciones intermedias como la creación del área de desarrollo e implementación requirió de planes de contingencia urgentes, esto ocurrió en marzo del 2013.

La expansión del instituto hacia otras sedes, provocó nuevos requerimientos y por ende se recurrió a nuevos planes de contingencia para aplacar o solucionar estos que la expansión provocaba.

2.1.4. FUNDAMENTOS TEÓRICOS

2.1.4.1. CONTINGENCIA

“Se conoce como contingencia (del latín contingentia) a un evento que es probable que ocurra pero del cual no se tiene la certeza de que vaya a ocurrir. Una contingencia es por lo tanto un suceso posible con mayores o menores probabilidades de ocurrir.” (Cortez, 2012)

Por medio de los planes de contingencia se planea poder evaluar las situaciones imprevistas que pueden surgir en el área de tics

2.1.4.2. CONTINGENCIA INFORMÁTICA

Se define la Seguridad de Datos Informáticos como un conjunto de medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre. Se ha considerado que para la empresa, la seguridad es un elemento básico para garantizar su supervivencia y entregar el mejor servicio a sus clientes, y por lo tanto, considera a la Información como uno de los activos más importantes de la Organización, lo cual hace que la protección de esta, sea el fundamento más importante de este Plan de Contingencia (Teckelino., 2011).

Con el fin de poder realizar una evaluación de planes de contingencia es necesario utilizar el ámbito informática para conseguir determinar la situación del área de tics

2.1.4.3. AUDITORIA INFORMÁTICA

Conjunto de procedimientos y técnicas para evaluar y controlar, total o parcialmente, un sistema informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existentes en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente (Parra Galvis, 2012)

Dado que la auditoria informática engloba objetivos específicos dentro de los cuales está la evaluación de la suficiencia de los planes de contingencia, este trabajo genera un plan de mejoras a las contingencias de las actividades más frecuentes realizadas por el área de tics.

2.1.4.4. SERVIDORES WEB

Un servidor Web es almacenar los archivos de un sitio y emitirlos por Internet para poder ser visitado por los usuarios. Básicamente, un servidor Web es una gran computadora que guarda y transmite datos vía Internet (Sierra, 2013).

Son tres los servidores que están instalados en el área de tics, por su continuo acceso es meritorio que tengan un plan de contingencia definido, por lo que es uno de los temas a evaluar.

2.1.4.5. PROGRAMACIÓN

Se conoce como programación en ciencias de la computación a los pasos que se abordan para crear el código fuente de un programa informático. De acuerdo con estos pasos, el código se escribe, se prueba y se perfecciona (CARDONA, 2011).

Debido a que una de las actividades del departamento de tics es la atención a los desarrollo de programas, esto se lo realiza mediante la programación en varios lenguajes de programación los que son asignados según la disponibilidad de los programadores.

2.1.4.6. IMPLEMENTACIÓN

Una implementación es la instalación de una aplicación informática, realización o la ejecución de un plan, idea, modelo científico, diseño, especificación, estándar, algoritmo o política (O'Higgins, 2012).

Es necesario tener en cuenta que un equipo necesita varios programas que estén acorde a la necesidad del doncente para lo cual se procede a implementar las herramientas necesarias y poder cumplir las demandas de los usuarios

2.1.4.7. SERVICIOS INFORMÁTICOS

Un servicio de tecnologías de la información es un conjunto de actividades que buscan responder a las necesidades de un cliente por medio de un cambio de condición en los bienes informáticos (llámese activos), potenciando el valor de estos y reduciendo el riesgo inherente del sistema. (Morales, 2012)

Con el fin de tener una idea clara de los servicios físicos que provee el área de permite tener una idea en cuanto a mantenimiento físico o lógico se refiere

2.1.4.8. SOPORTE TÉCNICO (HELP DESK)

"Es aquella existencia que se le brinda a un usuario. Este puede ser de 2 formas el soporte técnico presencial y el soporte técnico de distancia" (castro, 2013)

Es lo principal en la solución física en cuanto a problemas informáticos se refiere y requiere un procedimiento de atención tratada como una cola. Esta solución es a problemas de software como virus e instalación de programas y problemas de equipos en mantenimiento y/o reparaciones menores.

Dada la característica técnica-informática de esta investigación, aquí se han expuesto los conceptos que permiten identificar la temática y los términos en la que se desarrollan los planes de contingencia que requiere el área de tics del Instituto Tecnológico Bolivariano.

2.1.4.9. CONCEPTOS OPERATIVOS DEL ÁREA DE TICS

AMENAZA

Para realizar un análisis de los riegos, se procede a identificar los objetos que deben ser protegidos, los daños que pueden sufrir, sus posibles fuentes de daño y oportunidad, su impacto en la compañía, y su importancia dentro del mecanismo de funcionamiento.

Posteriormente se procede a realizar los pasos necesarios para minimizar o anular la ocurrencia de eventos que posibiliten los daños, y en último término, en caso de ocurrencia de estos, se procede a fijar un plan de

INTERNET

El nombre Internet procede de las palabras en inglés Interconnected Networks, que significa “redes interconectadas”. Internet es la unión de todas las redes y computadoras distribuidas por todo el mundo, por lo que se podría definir como una red global en la que se conjuntan todas las redes que utilizan protocolos TCP/IP y que son compatibles entre sí. (Rivera Ramírez, 2011)

El internet es la herramienta más utilizada ya que por medio de un sistema informático (Sistema de Gestión Académica)se está al tanto de los procedimientos que realizan los docentes se hacen comunicaciones

SISTEMAS INFORMÁTICOS

(Camazón, 2012) Certifica que Un sistema informático es un conjunto de elementos que es tan relacionado entre sí y en el que se realizan tareas relacionadas con el tratamiento automático de la información.

Un Sistema Informático utiliza ordenadores para almacenar los datos de una organización y ponerlos a disposición de su personal. Pueden ser tanto humanos, contabilidad, producción, inventario, etc. Los sistemas de información tienen muchas cosas en común. La mayoría de ellos están formados por personas, equipos y procedimientos. Al conjugar una serie de elementos como hombres y computadoras se hace imprescindible tomar medidas que nos permitan una continuidad en la operatividad de los sistemas

para no ver afectados los objetivos de las mismas y no perder la inversión de costos y tiempo.

PROGRAMA

Un programa informático o programa de computadora es una secuencia de instrucciones, escritas para realizar una tarea específica en una computadora Este dispositivo requiere programas para funcionar, por lo general, ejecutando las instrucciones del programa en un procesador central

ADMINISTRACION

La palabra administración proviene del latín: ad significa dirección, tendencia, minister significa subordinación, obediencia.

Es decir cumplimiento de una función bajo el mandato de otro, es el proceso cuyo objetivo es la coordinación eficaz de recursos de un grupo social para cumplir sus objetivos con mayor productividad..

(Ramirez, 2014)

PARCHE

(Valeria, 2014) Es un programa que modifica de forma temporal o permanente una aplicación para eliminar limitaciones o candados impuestos en los mismos originalmente

Generalmente un parche sirve exclusivamente para una determinada aplicación (incluso sólo para una determinada versión de esa aplicación).

El aseguramiento de la información

Para la correcta administración de la seguridad de la información, se deben establecer y mantener acciones que busquen cumplir con los tres requerimientos de mayor importancia para la información, estos son [5]:

• **Confidencialidad:** Busca prevenir el acceso no autorizado ya sea en forma intencional o no intencional a la información. La pérdida de la confidencialidad puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la organización.

• **Integridad**: Busca asegurar: o Que no se realicen modificaciones por personas no autorizadas a los datos o procesos. o Que no se realicen modificaciones no autorizadas por personal autorizado a los datos o procesos. o Que los datos sean consistentes tanto interna como externamente.

• **Disponibilidad**: Busca asegurar acceso confiable y oportuno a los datos o recursos para el personal apropiado. Diferentes organizaciones internacionales han definido estándares y normas que apoyan en diferente medida el cumplimiento de los requerimientos indicados anteriormente. A continuación se detallan los de mayor utilización a nivel mundial, y que fueron tomados como base para el modelo propuesto.

Estándares de calidad

ISO Es un estándar para la administración de la seguridad de la información, e implica la implementación de toda una estructura documental que debe contar con un fuerte apoyo de la alta dirección de cualquier organización. Este estándar fue publicado por la International Organization for Standardization (ISO) en diciembre de 2000 con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones. Esta norma internacional ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

COBIT Acrónimo de “Control Objectives for Information and related Technology” (Objetivos de Control para la Información y Tecnologías Relacionadas), es un estándar desarrollado por la Information Systems Audit and Control Foundation (ISACA), la cual fue fundada en 1969 en EE.UU., y

que se preocupa de temas como gobernabilidad, control, aseguramiento y auditorias para TIC.

Actualmente tiene más de 60.000 miembros en alrededor de 100 países. Esta organización realiza eventos y 239 conferencias, y desarrolla estándares en TI de gobierno, aseguramiento y seguridad, siendo COBIT el más importante. En los últimos 5 años ha cobrado fuerza debido a que fue desarrollado en específico para el ámbito de las TIC.

Por qué implementar controles

Un reporte de Deloitte muestra como en los 12 meses previos al estudio, distintas compañías de gran tamaño enfrentaron crisis de seguridad de información.

Como conclusiones del informe se muestra que el 69% de los participantes dijo estar “confiado o muy confiado” sobre la efectividad de la organización para enfrentar retos de seguridad provenientes del exterior. Sin embargo, sólo el 56% mostró esta confianza para enfrentar las amenazas internas.

El estudio también muestra que las empresas, si bien están constituidas por activos físicos -edificios e infraestructura-, y activos de información - contenido digital-, muchas de las compañías administran los riesgos de seguridad físicos y de información como entidades separadas y distintas, lo que puede implicar pérdida de oportunidades.

Adicionalmente, las empresas deben evitar una serie de riesgos de seguridad, entre los que incluyen robo de identidad, fuga de información, fraude y otros, por lo que es necesario contar con un marco de gobernabilidad en relación a la seguridad de la información.

Del informe se desprende la necesidad de una estrategia de seguridad en la información alineada con las iniciativas de las organizaciones. De acuerdo con la encuesta, el 54% de las empresas cuenta con una estrategia, el 20% planea

hacerlo en los próximos dos años; en tanto, el 17% considera que la falta de esta estrategia es una de las principales barreras para lograr seguridad en la información

De esta forma, uno de los puntos más importantes para definir controles de seguridad de la información, es instaurar políticas claras al respecto, que establezcan un marco regulatorio para las actividades que deben ser llevadas a cabo en este contexto.

Parámetros para establecer Políticas de Seguridad de la Información (PSI)

La implementación de Políticas de Seguridad de la Información es un proceso técnico y administrativo que debe abarcar a toda la organización, por ende, debe estar avalado y contar con un fuerte apoyo de la dirección y/o máxima gerencia, ya que sin este apoyo, su implementación será más compleja e incluso puede fracasar.

Es importante que al momento de formular las políticas de seguridad de la información, se consideren por lo menos los siguientes aspectos

o Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa. Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.

Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad. Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en proteger los activos críticos en su área.

Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

Razones que impiden la aplicación de las políticas de seguridad informática. Se debe ser capaz de convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática, sino los esfuerzos de su implementación pueden ser desperdiciados

Otros inconvenientes lo representan los tecnicismos informáticos y la falta de una estrategia de mercadeo por parte de los Gerentes de Informática o los especialistas en seguridad, que llevan a los altos directivos de las empresas a no comprender exactamente la razón o motivos de las inversiones.

Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen información sensible y por ende su imagen.

Ante esta situación, los encargados de la seguridad deben confirmar que las personas entienden los asuntos importantes de la seguridad, conocen 243 sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

Si se quiere que las políticas de seguridad sean aceptadas, deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencia en las proyecciones y utilidades de la compañía.

Finalmente, es importante señalar que las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que

facilitan la formalización y materialización de los compromisos adquiridos con la organización.

Oficial de Seguridad de la Información

(Farias-Elinos, 2012) La falta de una figura encargada de coordinar, planear y promover las actividades que tengan que ver con la parte de seguridad informática genera una situación que se ve reflejada en el crecimiento de problemas de seguridad que se presentan dentro de las instituciones, tales como intrusiones, robo de información, problemas de virus, entre otros

Este rol puede ser perfectamente desempeñado por una persona que esté certificada en temas de seguridad de la información (no técnica sino de administración o auditoria), sin embargo, dado el pequeño número de profesionales que obtienen este tipo de certificaciones y atendiendo a la realidad de las organizaciones, en general esta labor es cubierta por un profesional (no necesariamente informático) que se ha especializado en esta área.

las alertas, así como de proponer y definir esquemas que reduzcan los incidentes de seguridad que se presenten. El OSI tiene la función de brindar los servicios de seguridad en la organización, a través de la planeación, coordinación y administración de los procesos de seguridad informática, así como difundir la cultura de seguridad informática entre todos los miembros de la organización.

Implementar y Estructurar Controles.- Con el propósito de enfrentar correctamente los procesos de auditoria y a la vez para satisfacer un adecuado nivel de control interno en las actividades de TIC, se deben diseñar controles, de manera que ellos abarquen a todos los procesos que se manejan por medio

de las TIC en una organización. En todo este proceso el OSI juega un papel de relevancia, puesto que con su experiencia se pueden realizar estas implementaciones en forma adecuada y con la relevancia que la organización requiere.

En sí, los controles deben estar construidos en base a áreas (procesos) y objetivos de control de los cuales se deben desprender las actividades y finalmente los controles en si. Por ejemplo la norma ISO/IEC 27002 describe 39 objetivos de control. Sin embargo, otras normas o estándares como ISO 17799, ITIL y COBIT proponen un número distinto de controles.

De manera de apoyar la implementación del modelo propuesto y de modo de hacer práctico el proceso de estructurar e implementar controles, el modelo entrega una estructura, con una base de 85 objetivos de control de los cuales nacen 120 controles generales para TIC. Esta base de controles debe ser ajustada según el ámbito de la organización y los alcances de sus actividades en TIC.

Estos controles han sido establecidos conforme al estudio de los estándares antes citados, considerando especialmente las indicaciones de ISO 17799 e ISO/IEC 27002), y pretenden ser una guía para quien estime su activación. Es importante recalcar que los controles en si no bastan para tener un correcto gobierno de TI, ya que ello solo se puede alcanzar

Actualmente esta base de controles se encuentra operativa en algunas empresas de Chile (se reserva su identidad, por políticas de seguridad). Estos controles han sido revisados y aprobados en su implementación por distintas entidades de auditoria de renombre nacional e internacional, lográndose, por ejemplo, la reducción de las indicaciones.

La aplicación de esta base de controles en algunas empresas de Chile ha permitido mejorar los resultados obtenidos en procesos de auditoria de

estados financieros anuales, disminuyendo considerablemente las indicaciones hacia áreas de TIC.

Algunas mediciones con base ISO muestran importantes mejoras en niveles de seguridad al implementar estos controles, midiendo aspectos tales como implementación de PSI, organización de la seguridad, gestión de activos, seguridad del recurso humano, gestión de continuidad, gestión de comunicaciones y operaciones, destacándose que al implementar PSI se alcanza una diferencia mayor a 20 puntos porcentuales sobre el promedio de empresas Chilenas evaluadas, otro ejemplo es la gestión sobre la continuidad operaciones en donde se alcanza una diferencia de poco mas de 17 puntos porcentuales sobre el promedio.

No obstante el nivel de mejora respecto a empresas del mismo sector y el buen nivel del manejo de riesgo, al comparar los resultados con el sector bancario, en algunos casos los resultados están bajo 30 puntos porcentuales, esto debido a que el sector bancario ha realizado los mayores esfuerzos en este sentido, dado lo significativo de este aspecto en sus actividades. Las organizaciones que tienen mayor interés en asegurar y demostrar menor riesgo son las instituciones y organizaciones bancarias-financieras [10] (el activo de información en este caso, puede efectivamente determinar la continuidad de sus operaciones). Ellas están en obligación de implementar estándares y metodologías de clase mundial que permitan el resguardo a sus clientes (como los citados anteriormente), en contrapuesto a una Pyme, que si bien tiene el foco comercial bien establecido, está claramente muy por debajo de esta línea de confianza respecto a la seguridad de sus TIC, ya que no tiene este nivel de obligación, que sin embargo, puede ser un diferenciador de mucha relevancia. La aplicación del esquema de controles que presenta este

Modelo puede ser aplicado en organizaciones grandes y pequeñas, en las cuales, los resultados de su implementación retornarán beneficios de seguridad, confiabilidad, integridad y disponibilidad de la información que

resguarde y/o utilice por medio de TICs. Esto, junto al giro de la organización puede significar un aumento de confianza de sus clientes respecto a la información que de ellos se maneja, y pudiera en definitiva ser un aspecto "diferenciador" de otras organizaciones.

Cada control o grupo de controles forma parte de su objetivo de control, del cual se desprenden las actividades de control que dan origen al control en sí. A su vez cada objetivo forma parte de una agrupación mayor que es el proceso. Los procesos están agrupados en 7 grandes áreas que son: Mantención, Seguridad, Operaciones, Desarrollo, Acceso General, Recuperación de Desastres, y Computadores. Por ejemplo, para el proceso de Seguridad, uno de los objetivos de control considerados es Toda la información es respaldada en forma oportuna y adecuada; uno de los controles asociados a este objetivo es Monitoreo de errores en respaldos en servidores.

La tarea que debe asumir cada organización, conforme a su propia realidad es la de identificar cuál es la evidencia que cubre al respectivo control, lo que es particular y propio a cada organización; inclusive es altamente probable que uno o varios controles no apliquen al contexto de la organización. Ante esta situación lo que se recomienda es mantener el control, pero indicar en su evidencia o actividad que éste, dado el contexto particular de la organización "no aplica". Junto a esto se debe realizar lo indicado por COBIT y COSO en base a definir si los controles serán de efecto primario o secundario para los estados financieros de la organización, lo cual, permitirá dar la criticidad a cada uno de ellos.

La concreción de las tareas de control se pueden plasmar en un solo documento, en el cual se identifique la lista de procesos, objetivos de control y controles de TIC, la cual será la base de revisión que debe ser monitoreada con la periodicidad que defina la organización donde la evidencia de cada control constituirá el elemento central que probará la efectividad del control

La actividad anteriormente señalada debería ser realizada por el OSI y/o por un auditor interno o externo, además se recomienda realizar el proceso en conjunto con la alta dirección y con él área de finanzas a fin de evaluar que controles serán clasificados como primarios y secundarios en orden a alinearse conforme a la normativa COSO y determinar así cuáles son los reales impactos en los estados financieros. Así se podrá dar relevancia y prioridad a los controles. En todas estas actividades de definición de controles debería participar activamente el OSI de forma tal que pueda ser el interlocutor válido ante procesos de auditoría interna o externa.

Modelo de Control de Riesgos de Seguridad

Hoy en día son múltiples los riesgos asociados a que equipos y sistemas de información y comunicaciones no cuenten con controles de seguridad. Las amenazas en las TIC son globales, y están repartidas en distintos niveles de criticidad según sea la orientación y el ámbito de su utilización. Preocupante es para grandes, medianas y pequeñas organizaciones el espionaje industrial, los ladrones de información, la interrupción de servicios y las fallas críticas en la infraestructura y sistemas centrales de información. Este modelo puede ser perfeccionado y modificado en el futuro dado que su estructura se debe ajustar a los constantes cambios que surgen de las organizaciones como sistema dinámico.

La particularidad del modelo que se presenta a continuación reside en su aspecto operativo y práctico, puesto que se considera su estructuración, formación e implementación bajo dos grandes fases.

- Fase de Elaboración
- Fase de Aplicación

Estas fases contemplan el conjunto de actividades que de ellas se desprenden y están ligadas mediante la secuencia de actividades que es necesario desarrollar a fin de elaborar y aplicar correctamente el modelo.

Este modelo considera los principales elementos incluidos en las diversas normas y estándares internacionales relacionados con la seguridad de la información, por lo que creemos que apoya la concreción de un "Gobierno de TIC", lo que a su vez abarca un aspecto mayor al que su diseño se orientó inicialmente, ya que esto implica que no solo cubre temas de seguridad y de riesgos, sino a que al mismo tiempo apoya a lograr aspectos de estructura organizacional, descripciones de cargo y tareas, definiciones de misión y visión, no solo a nivel gerencial, sino que a nivel de cada área de TIC. (Salazar Burgos, 2014)

Gracias a este modelo de control de riesgos nos es posible dividir en fases cualquier eventualidad dependiendo de su causa y nivel de criticidad y poder reaccionar apropiadamente.

Aporte del Modelo De Seguridad

Este modelo se apoya en el análisis de los estándares y normas de la seguridad de la información presentada, junto a los alcances y formas de implementación, más el rol del OSI y la implementación de controles. Su principal aporte es ser un facilitador en la implementación y/o aplicación de la seguridad de la información para TIC en cualquier tipo de organización.

La estructura que presenta el modelo se basa sobre la implementación práctica y concreta relacionada con las actividades que permitan dar seguridad a la organización, la cual, en base a sus propias necesidades, lineamientos y perspectivas de negocio, busca mantener su información asegurada.

Otro aspecto importante que aporta este modelo, es que, por su presentación simple puede ser correlacionada sin mayor dificultad con las actividades que realiza cualquier tipo de organización, de manera que ella logre asegurar la información en conformidad a la realidad de TIC que disponga.

En la implementación del modelo se debe tener conocimiento de las funciones, tareas, actividades y diseño relacionadas con cada una de las etapas, por lo

cual, se enfatiza en el rol de un OSI, ya que con su aporte la 252 organización podrá estructurar de forma adecuada su seguridad.

El rol del OSI es relevante en el control, monitoreo y seguimiento de los planes de acción, ya que esto permite el ciclo continúo de perfeccionamiento y de vida del modelo.

El presente modelo, avalado en los estándares presentados en este artículo, pretende ser una solución y aporte en la implementación de la seguridad de la información de cualquier organización.

2.1.5. ANTECEDENTES REFERENCIALES

Situación en la región: Universidad de Monterrey

A continuación las contingencias informáticas que se suscitan en la Universidad de Monterrey y sus métodos prácticos para remediar situaciones emergentes.

El **respaldo de la información** que tenemos almacenada en el disco duro de la Computadora de la oficina o en el servidor de la red, es el último recurso en caso De que ocurra alguna de las siguientes situaciones típicas:

- Falla del disco duro
- Fallas Interrupciones de energía
- Energía no regulada
- Errores del personal de operación
- Errores de programación (sobre todo al modificar alguna aplicación, Incompatibilidades)
- Inundación, incendio, desastre
- Problemas climatológicos
- Infecciones con virus
- Robos

Si desea conocer más información sobre virus computacionales, consulte el

Documento *¿Qué es un virus computacional y qué hacer en caso de virus?* Que Se encuentra en el material de apoyo del presente módulo.

Estas situaciones ocurren con más frecuencia de lo que pensamos, por lo que Debemos contar con un respaldo de la información reciente, de manera que no Se pierda toda la información en caso de que ocurra alguna sorpresa. La ubicación de las computadoras deberá determinarse para evitar que estén en Lugares donde podría presentarse un riesgo para la integridad del equipo.

Deberán evitarse los siguientes lugares:

- Bajo los ductos de aire acondicionado, ya que podría haber condensación de agua o fuga.
- Aparatos de A/A, por la misma condensación.
- Tuberías que atraviesan la sala de cómputo, por el techo: agua potable; Drenaje sanitario; drenaje pluvial.
- Alcantarillas, drenaje pluvial de las azoteas o lugares bajos.
- En sótanos que se pueden inundar por una tormenta.

Obviamente se debe contar con alimentación de energía eléctrica regulada y tener instalada una tierra efectiva, para disminuir la posibilidad de altos voltajes.

Los Tipos de información a respaldar en la universidad d ‘emionter son:

- Aplicaciones institucionales, Nóminas, contabilidad, ventas, pagos, almacén, etc.

Sistemas de información ejecutiva

Esta información tiene su fuente en los sistemas institucionales ya que es una consolidación. La página web, es la imagen de la institución.

Los datos que residen en los discos duros de los usuarios, son producto de los análisis, investigaciones, proyectos, presentaciones, entrenamiento, etc. Por lo que se debe analizar su importancia y asegurar el respaldo periódico.

Programas, son los desarrollados internamente, porque son propiedad intelectual, están sujetos a derechos de autor. Este software debe de respaldarse, tanto los programas fuente como los objeto Paquetes adquiridos,

como Office, administración de proyectos, etc. o Software del sistema operativo como el Windows, SQL, Visual Basic, etc.

Documentación

Se debe analizar la forma de recuperar la información en papel y en caso de requerirse un respaldo se puede utilizar la opción de imagen. Se puede utilizar equipo de escáner para obtener una imagen de la información crítica y respaldarla en un disco compacto.

- Legal
- Documentación de los sistemas
- Políticas
- Contratos
- Escrituras
- Demandas
- Derechos de autor
- Acciones de empresas

En algunos casos se puede optar por tener el respaldo en una bóveda externa Que podría ser un banco.

Procedimientos

Es importante asegurar que los procedimientos operativos se respalden también, De preferencia en medios electrónicos, ya que representan las prácticas que la Organización ha ido desarrollando conforme pasa el tiempo y representan una Ventaja competitiva.

Entre otros, los procedimientos que se deben respaldar son:

- Procedimientos de recuperación en caso de desastre
- Procedimientos operacionales
- Procedimientos administrativos
- Procedimientos de reparación (manuales de proveedores)
- Procedimientos donde se establece la configuración de las redes

Parámetros y configuraciones

Es importante respaldar los parámetros de los sistemas de control de acceso, como:

Estrategias de respaldo

El área de soporte técnico deberá establecer una estrategia de respaldos, Dependiendo del tipo de información y de la volatilidad de la misma. Una recomendación muy utilizada consiste en:

Respaldo total del disco y sistema operativo (mensual)

1.1 Depende de la volatilidad de la información.

1.2 Depende de las modificaciones (nuevas versiones, parches, rotación de cuentas de acceso, etc.)

Respaldo total de la información (semanal)

2.1 Los fines de semana se obtiene un respaldo de información.

2.2 En algunos casos se podría también respaldar los directorios de usuarios y privilegios de acceso.

3. Respaldo diario de bases de datos

El respaldo diario incremental es el más recomendado, si la tecnología lo permite.

Enviar una copia de los respaldos a bóveda externa (semanal)

Es de vital importancia contar con un respaldo en bóveda externa, ya que será el último recurso en caso de un desastre en el centro de cómputo.

Almacenamiento de cintas

La bóveda donde está la "*cintoteca*" es el lugar donde están los archivos históricos de la organización y se debe garantizar un mínimo de requisitos de seguridad como:

- Cintas Grabadas durante tres meses.
- La bóveda donde se almacenan las cintas debe estar protegida con una cámara De video conectada al centro de control de seguridad
- Deberá contar con detectores de humo y movimiento, en muchos casos Se justifica tener un sistema de extinción automática, deberá

asegurarse. Con el proveedor de la media magnética si requiere algunas condiciones. Especiales de humedad y temperatura.

- Uno de los respaldos totales deberá ser almacenado en una bóveda Externa, con el propósito de disminuir el impacto en caso de un desastre. Se recomienda tener un proceso semanal, utilizando una oficina protegida Que esté fuera de los terrenos de la oficina central. El uso de los servicios De traslado de valores es una buena opción para asegurar que esa actividad se efectúe sin falta.

Respaldo de información

Normalmente esta actividad debe ser responsabilidad del mismo usuario de una computadora, sin embargo, dependiendo de las políticas de seguridad, algunas empresas activan la facilidad para que el operador de la red respalde su información cuando la computadora esté encendida.

La frecuencia de respaldo dependerá de la volatilidad de la información, lo usual es una vez por semana.

Sería muy triste que cuando se requiera usar el respaldo, éste no funcionara. Esto suele suceder de vez en cuando, debido a malos procedimientos de respaldo, por lo que recomendamos seguir las siguientes instrucciones:

- Asegurarse que los respaldos sean recuperables, mediante una prueba De cinta.
- Asegurar la compatibilidad de los dispositivos, ya sean cartuchos, cintas, Disquetes o discos compactos. Es lamentable contar con respaldos pero No disponer del equipo para recuperarlos.
- Otra situación frecuente es cuando el respaldo no se completó, por Control de acceso a nivel excelencia. Se recomienda instalar una voz general

Desastres informáticos

Anteriormente sólo los sistemas de nómina, contabilidad, almacén, etc., estaban soportados y algunas empresas no sufrían un gran impacto si tenían interrupciones prolongadas de servicio (más de 4 días). Una recaptura de los

datos solucionaba los problemas, sólo era cuestión de tiempo.

Sin embargo, las organizaciones en la actualidad dependen cada vez más de sus servicios de información ya que han buscado mejorar su servicio al ciudadano y hacer eficientes sus operaciones. Un desastre en sus oficinas no permitiría la continuidad del negocio.

El gobierno electrónico es el mandatario para que toda organización tenga Planes de recuperación en casos de desastres, para evitar que un evento de ese tipo afecte los resultados financieros.

Un ejemplo muy claro es el área de protección civil, donde los servicios de información a la población durante un fenómeno meteorológico son tan importantes que en caso de fal as podrían significar hasta pérdidas de vidas.

Otro ejemplo es el abastecimiento de medicinas. En caso de que una institución de seguridad social no tuviera la disponibilidad de reportar por medio de los servicios de cómputo conectados a las grandes empresas farmacéuticas, la escasez de algunas medicinas, sería crítica para la atención de los pacientes.

No olvidemos de las empresas que dependen del gobierno para proporcionar Servicios de energía eléctrica o de abastecimiento de petróleo. En estos casos,

Los servicios de cómputo y telecomunicaciones son críticos y deben estar disponibles las 24 horas del día, los 7 días de la semana, durante los 365 días del año.

Situación local

A continuación las contingencias informáticas que se suscitan en la Universidad Espol y sus métodos prácticos para remediar situaciones

Seguridad informática

Como la ESPOL es una institución donde la Tecnología de la Información tiene un uso intensivo, el Centro de Servicios Informáticos ha implementado las siguientes seguridades informáticas:

- A nivel de la red de datos de la ESPOL, se tiene 2 firewalls para proteger el perímetro de la red y los servidores principales de la ESPOL, con lo cual solo se tiene acceso a las aplicaciones permitidas
- Antivirus en las computadoras de ESPOL para protección de las diferentes amenazas de virus que existen en la actualidad. Adicionalmente, el software antivirus tiene servicios adicionales como: firewall, protección contra malware y phissing
- Servidor AntiSpam para la protección de los buzones de mensajes de las cuentas de correo electrónico. Este es un software de código abierto
- Cuenta electrónica única, la cual permite el acceso usando un solo usuario y clave a los diferentes servicios proporcionados por ESPOL. Adicionalmente, el acceso a las cuentas tienen configuradas políticas de acceso, por ejemplo, si se ingresa erróneamente la contraseña de una cuenta en más de tres ocasiones, la cuenta se bloquea por un período de 2 horas
- Certificados de seguridad (adquiridos a e-sign, certificadora internacional) para los sitios web que requieren seguridad adicional en la comunicación: Sitio Web académico, Sitio de Creación de Cuentas, Sitio de WebMail
- Seguridad a nivel de las aplicaciones institucionales, cada usuario solo tiene acceso a las opciones e información necesarias para realizar su trabajo. Esta seguridad es implementada a través de perfiles de trabajo tales como director, coordinador, asistente, etc. Cada perfil tiene asignados los permisos para acceder a una serie de opciones de cada sistema. Por lo tanto cada usuario de un sistema tiene asignado un perfil, que le permite usar solo unas determinadas opciones. Existen perfiles de administrador para quienes manejan todas las opciones de los sistemas.
- Monitoreo de registros de las transacciones (log de transacciones) de las aplicaciones. Se tiene registros de las transacciones críticas que

actualizan datos, en cual se guarda fecha, hora, usuario de quien ejecuta la transacción.

- Restricciones en el acceso físico del hardware de los equipos que almacenan información crítica de la información.

CAPITULO III

METODOLOGIA

En este capítulo se expondrá la metodología procedimiento y etapas que se utilizaran para analizar el problema.

3.1 OBJETO DE ESTUDIO

El presente trabajo de investigación se realiza en el Instituto Superior Tecnológico Bolivariano de Tecnología, cuya actividad inicia el 12 de octubre de 1999 Cuyo objeto social es el Sistema de Educación Superior en el Ecuador se encuentra en un proceso de fortalecimiento de posiciones y principios que tiene como objetivo garantizar la generación, asimilación y transferencia de conocimientos con intencionalidad social concreta y en función del desarrollo y la mejora para el Buen Vivir de los Ecuatorianos.

Consciente de estos retos y desafíos, el Instituto Superior Tecnológico Bolivariano de Tecnología, asumiendo la responsabilidad que emana del encargo histórico y social que le corresponde como una Institución de Educación Superior, ha continuado trabajando incansablemente por la mejora continua de todos sus procesos sustantivos, con un modelo de gestión que garantiza la consolidación de los objetivos y estrategias del Plan Nacional de desarrollo para el Buen Vivir.

La misión del tecnológico es “Formar profesionales técnicos y tecnólogos que aportan con excelencia académica al crecimiento global sostenible, capaces de satisfacer competencias laborales que demandan los sectores productivos y sociales. “

Su visión es **“**Ser una Institución de Educación Superior acreditada con bases filosóficas, propositivas, científicas e innovadoras; formando profesionales emprendedores con sólidos conocimientos tecnológicos que aporten al desarrollo global, sustentable y protección al medio ambiente. **“**

Área de Tics

Las Tecnologías de la Información y la Comunicación, también conocidas como TIC, son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Abarcan un abanico de soluciones muy amplio. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes

El área de TICS esta conformado por las siguientes personas:

Lcda. Tatiana Tapia Bastidas ,Mae, PhD	Directora de Tics
Tnlgo. Nelson Villacres	Jefe de soporte Técnico
Ing. Daniel Navarrete	Soporte Aplicativo y Hardware
Ing. Andrea Aquino	Soporte Aplicativo y Hardware
Ing. Soraya Gallegos	Jefe de Programación
Ing. Juan José Urgirles	Analista Programador
Anl. Olga Castillo	Analista Programador
Ing. Rene Cardona	Programador web
Tnlgo. Adriana Peñafiel	Diseñadora Grafica

3.2. TIPOS DE METODOLOGÌAS DE INVESTIGACION

- Exploratorio
- Descriptivo
- Explicativo
- Comparativa

(Tancara G. C., 2013) Afirma que Cada uno de estos niveles de Metodologías implica diversos grados de profundidad y, en consecuencia, diferentes exigencias y dificultades metodológicas. Las investigaciones de nivel explicativo son mucho más complicadas que las descriptivas y presuponen un mayor nivel de parte del investigador. Además cada una de ellas es acumulativa, es decir una investigación descriptiva, lo es también, en algún grado exploratorio y una explicativa es exploratoria, descriptiva y clasificatoria entre otras.

Por lo que a continuación se explican los tipos de metodologías que se utilizaran en esta investigación para analizar el problema que se ha encontrado.

3.2.1. INVESTIGACIÓN EXPLORATORIA

(Brouyere, Investigación Exploratoria, Descriptiva, Correlacional y Explicativa, 2014) Lo primordial es estudiar un tema o problema de investigación poco experimentado o que no ha sido abordado antes. Estos estudios nos permiten aumentar el grado de familiaridad con fenómenos relativamente desconocidos. En escasas ocasiones este tipo de estudio constituye un fin en sí, dado que por lo general determinan tendencias, identifican relaciones potenciales entre variables. Por tal motivo en general es la primera fase de una investigación y pocas veces es una investigación en sí misma.

Cuando no existen investigaciones previas sobre el objeto de estudio o cuando nuestro conocimiento del tema es tan vago e impreciso que nos impide sacar

las más provisorias conclusiones sobre qué aspectos son relevantes y cuáles no, se requiere en primer término explorar e indagar, para lo que se utiliza la investigación

3.2.2. INVESTIGACIÓN DESCRIPTIVA

(Brouyere, Investigación Exploratoria, Descriptiva, Correlacional y Explicativa, 2014) Estos estudios buscan explicar las propiedades importantes de personas, grupos, comunidades o cualquier anomalía que se ha sometido al análisis. En un estudio descriptivo se selecciona una serie de debates y se mide cada una de ellas independientemente, de forma tal de describir los que se investiga. Este estudio nos puede ofrecer la posibilidad de llevar a cabo algún nivel de predicción, aunque sea fundamental. Como aproximación a un aspecto de la realidad social, tenemos en primer lugar en el sentido más primordial las investigaciones de tipo descriptivo.

Este Consiste fundamentalmente en caracterizar un fenómeno o situación específica indicando sus rasgos más peculiares o diferenciadores. La descripción consiste en poder responder las siguientes cuestiones al final de la investigación.

Pregunta	Términos
¿Qué es?	Enunciado
¿Cómo es?	Propiedades
¿Dónde está?	Lugar
¿Qué actores están involucrados?	Actores
¿Qué elementos lo componen?	Composición

Se trata, de una enumeración en la que se hace una especie de inventario de las preguntas antes indicadas. Es una forma de producir información que puede ser utilizada para todo tipo de trabajos e investigaciones.

3.2.3. INVESTIGACIÓN EXPLICATIVA

(Brouyere, Investigación Exploratoria, Descriptiva, Correlacional y Explicativa, 2014) Explicar es siempre un intento de responder a los porqué... ¿Por qué algo sucede como sucede?, ¿por qué algo es cómo es?

Este nivel es el que estudia lo más profundo de la investigación social pero que, por ahora constituye todavía un sector escasamente desarrollado. Para ciertos, este nivel se identifica con los estudios de comprobación de hipótesis causales.

Para nosotros esta identificación no es totalmente válida puesto que la explicación, como nivel de conocimiento, tiene estos objetivos principales.

- Explicar la causa de un fenómeno, y/o
- Insertar el fenómeno en un contexto teórico, de modo que permita incluirlo en una determinada generalización.

Recopilar datos, descubrir hechos, encontrar situaciones o clasificar los fenómenos, pero otra es saber por qué ocurren, cuáles son sus factores determinantes, de dónde proceden, cómo se evoluciona en el nivel explicativo se intenta dar cuenta de la realidad o de hacerla comprender a través de leyes científicas o de teorías.

La teoría en la que se acoplan leyes constituye un sistema explicativo global que finaliza la comprensión de la realidad. Cuando el investigador se plantea la búsqueda de respuesta a algunos de los fenómenos y hechos de la vida actual y esto no es lo frecuente se está trabajando a nivel explicativo. Por tal motivo sólo es posible en los sectores más avanzados de la investigación, que en las ciencias sociales, todavía subdesarrolladas, son poco numerosos.

3.2.4. INVESTIGACIÓN COMPARATIVA

(Hurtado de Barrera, 2012) Su objetivo es identificar diferencias y semejanzas entre dos o más grupos o unidades de estudio. Se realiza con dos o más grupos, y su objetivo es comparar el comportamiento de uno o más eventos en los grupos observados. Requiere como logro anterior la descripción del fenómeno y la clasificación de los resultados. Está orientada a destacar la forma diferencial en la cual un fenómeno se manifiesta en contextos o grupos diferentes, sin establecer relaciones de causalidad.

La investigación comparativa tiene como objeto lograr la identificación de diferencias o semejanzas con respecto a la aparición de un evento en dos o más contextos

3.3. POBLACIÓN Y MUESTRA

Población

En la presente investigación la población está conformada por la totalidad de las personas que laboran en el Instituto Tecnológico Bolivariano la cual está integrada por

Muestra

Es únicamente el subconjunto de la población, dada la conformacion y tamaño de la poblacion, se aplica la encuesta sobre la totalidad de la misma.

Cuadro No.1 Universo y muestra del ITB

GRUPOS	Tamaño del grupo (N)	Tamaño de la muestra (n)	Tipo de muestreo	METODO TECNICA
Autoridades del área de tics	3	2	Aleatorio	Entrevista
Asistentes del área de tics	6	3	Aleatorio	Entrevista
Docentes	100	33	Aleatorio	Encuesta
Estudiantes	200	64	Aleatorio	Encuesta

Fuente: ITB Elaboración: El Autor

3.3.1 TIPO DE LA MUESTRA

Docentes titulares

Estudiantes que usan los laboratorios, numero de lab y maquinas, eso nos da el número de estudiantes que se consideran en la muestra

3.3.2 TAMAÑO DE LA MUESTRA

La fórmula para calcular el tamaño de la muestra es la siguiente:

$$n = \frac{N * Z_{\alpha}^{2} * p * q}{d^{2} * (N-1) + Z\alpha^{2} * p * q}$$

Cuadro No.2 Cálculo de la muestra del ITB

GRUPOS	Tamaño del grupo (N)	Porcentajes	Tamaño de la muestra (n)
Autoridades del área de tics	3	2 %	2
Asistentes del área de tics	5	3 %	3
Docentes	100	33 %	33
Estudiantes	200	62 %	64
	308	100 %	102

Fuente: ITB Elaboración: El Autor

N = Total de la población

Za2 = Si el nivel de confianza es 95%

p = Proporción esperada (50%)

q = 1 – p (en este caso 1 – 0,5)

d = Precisión (deseamos un 5%, osea 0,05

n = 102 Tamaño de la muestra total

Al considerar un error del 5% ósea 0.05, hay un Nivel de Confianza del 95% ósea 0.95, lo que contribuye a que los resultados sean más precisos.

3.4. MÉTODOS Y TÉCNICAS

3.4.1. TÉCNICAS E INSTRUMENTOS

Las técnicas para la recopilación de información para el sistema propuesto fue la exploración directa esta modalidad nos dará la facilidad de percibir la realidad del objeto de estudio.

Encuestas

“Las encuestas son entrevistas con un gran número de personas utilizando un cuestionario prediseñado. Según el mencionado autor, el método de encuesta

incluye un cuestionario estructurado que se da a los encuestados y que está diseñado para obtener información específica." (Malhotra, 2008)

Estarán destinadas a obtener datos de varias personas o de una parte representativa, estas permitirán conocer los interrogantes sobre la falta de procesos internos debido a una administración inestable y falta de un sistema de control de información. Ver ANEXO №3.

Entrevistas

"La entrevista es una de las técnicas comúnmente utilizadas ya que consiste en el proceso de comunicación entre personas, generalmente entre dos (entrevistador y entrevistado). Se obtiene la información de manera directa entre los sujetos." (Malhotra, 2008)

Se realizaron entrevistas a través de preguntas previamente formuladas con el propósito de obtener información de las personas involucradas directamente con el sistema en estudio. Ver ANEXO №4.

3.4.2. MÉTODOS

3.4.2.1. INDUCTIVO.-

''Es el razonamiento que, partiendo de casos particulares, se eleva a conocimientos generales. Este método permite la formación de hipótesis, investigación de leyes científicas, y las demostraciones. La inducción puede ser completa o incompleta. '' (Baena, 2003)

El objeto de estudio de la lógica inductiva es el estudio de las pruebas que permiten medir la probabilidad inductiva de los argumentos así como de las reglas para construir argumentos inductivos fuertes. ...

3.4.2.2. Deductivo.-

“Mediante ella se aplican los principios descubiertos a casos particulares, a partir de un enlace de juicios. El papel de la deducción en la investigación es doble:

a. Primero consiste en encontrar principios desconocidos, a partir de los conocidos. Una ley o principio puede reducirse a otra más general que la incluya.

b. También sirve para descubrir consecuencias desconocidas, de principios conocidos.” (Baena, 2003)

Es el procedimiento o camino que sigue el investigador para hacer de su actividad una práctica científica. El método hipotético-deductivo tiene varios pasos esenciales: observación del fenómeno a estudiar, creación de una hipótesis para explicar dicho fenómeno

CAPITULO IV

ANÁLISIS DE RESULTADOS

4.1. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

El presente capítulo se muestra los resultados obtenidos por medio de la aplicación del instrumento de recolección de datos a la población objeto de estudio, con la finalidad de analizar la Evaluación y mejoramiento del Plan de contingencia en el área de tics del Instituto Tecnológico Bolivariano

Se interpretaron los resultados con el fin de facilitar la comprensión de los mismos atendiendo a la problemática planteada, y a sus objetivos de estudio. Cada uno de los ítems se analizó de manera cualitativa y cuantitativa.

4.1.1. ANÁLISIS DE LA SITUACIÓN ACTUAL

4.1.2. ANÁLISIS DE LOS DATOS DE LA ENCUESTA

PREGUNTA 1

¿Existe un sistema computarizado, que le permita el control de los bienes informáticos?

Cuadro 1: Sistema Computarizado

Alternativas	Muestra	Porcentaje
SI	2	30%
NO	7	70%
TOTAL	9	100%

Elaborado por: Michael Mora

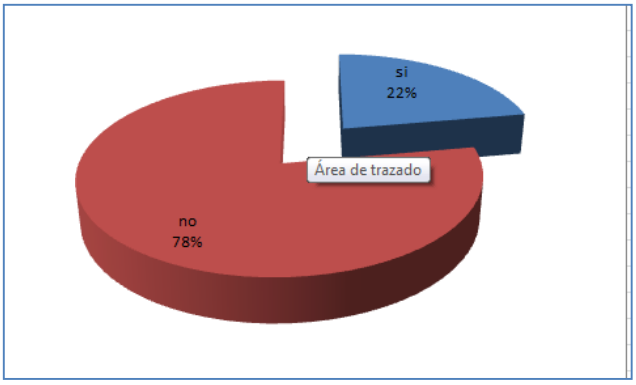

Grafico 1: Sistema Computarizado

Elaborado por: Michael Moral

Análisis

El 70% del personal respondió que NO existe ningún sistema computarizado de control de bienes informáticos, mientras el 30% del personal considera que si hay un sistema computarizado de inventario; es decir que el personal que labora asegura que no existe un sistema computarizado que permita llevar el control de la mercadería de la empresa; es importante resaltar que no existe es un sistema manual de control de bienes informáticos

PREGUNTA 2

¿Cree usted que se tiene suficientes usuarios con códigos de acceso remoto?

Cuadro 2: Acceso Remoto

Alternativas	Muestra	Porcentaje
SI	1	10%
NO	8	90%
TOTAL	9	100%

Elaborado por: Michael Mora

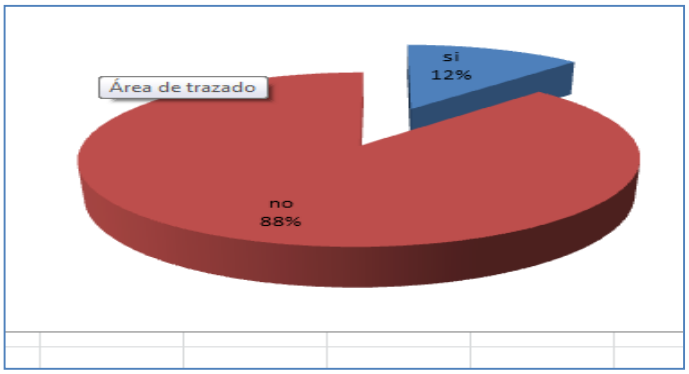

Grafico 2: Acceso remoto

Elaborado por: Michael Moral

Análisis

El 90% del personal respondió que NO existe suficientes usuarios que puedan dar soporte con el acceso remoto, mientras el 10% del personal considera que si hay la cantidad propia de personal; es decir que el personal que labora asegura que no existe suficiente personal que permita llevar el control de acceso seguro; es importante resaltar que si el responsable llegara a faltar puede dificultar las operaciones

PREGUNTA 3

¿Cree usted que los laboratorios están con las herramientas adecuadas para el rol de aprendizaje?

Cuadro 3: Rol de Aprendizaje

Alternativas	Muestra	Porcentaje
SI	4	40%
NO	5	60%
TOTAL	9	100%

Elaborado por: Michael Mora

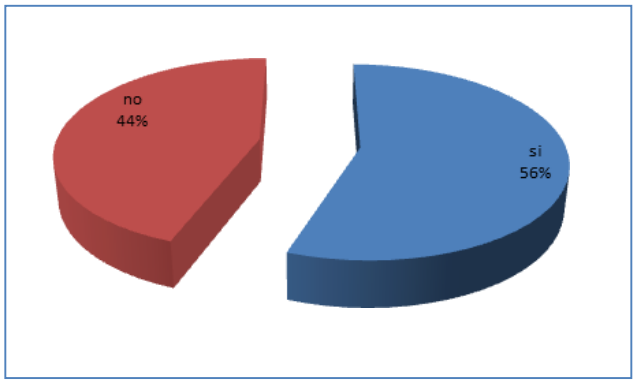

Grafico 3: Rol del aprendizaje

Elaborado por: Michael Moral

Análisis

El 56% del personal respondió que Si existe suficientes programas y aplicaciones para facilitar el aprendizaje, mientras el 44% del profesorado explica que aun necesitan más programas para facilitar la enseñanza; es decir que el personal que labora asegura existe suficientes herramientas para la enseñanza; es importante resaltar que si llegara a faltar alguna aplicación retrasaría las clases un día

PREGUNTA 4

¿Cuándo un usuario tiene un problema en el sistema, puede ser ayudado?

Cuadro 4: Ayuda en el Sistema

Alternativas	Muestra	Porcentaje
SI	9	100%
NO	0	0%
TOTAL	9	100%

Elaborado por: Michael Mora

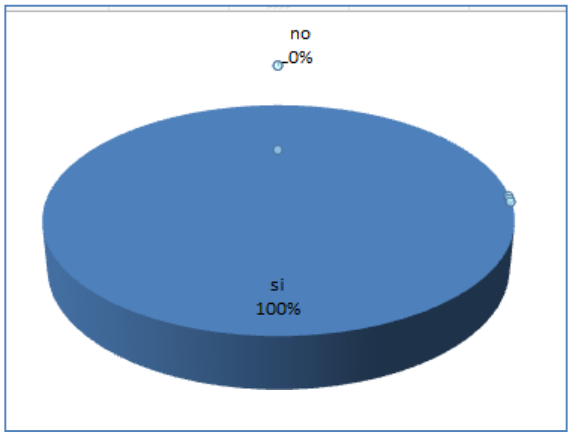

Grafico 4: Ayuda en el sistema

Elaborado por: Michael Moral

Análisis

El 100% del personal respondió que Si alguna inquietud en cuanto alguna duda con el sistema; es decir que el personal que labora asegura resolver cualquier duda con respecto al sistema

PREGUNTA 5

¿Usa usted los laboratorios de manera apropiada y dentro del tiempo estimado de clases?

Cuadro 5: Equipo del Laboratorio

Alternativas	Muestra	Porcentaje
SI	8	80%
NO	1	20%
TOTAL	9	100%

Elaborado por: Michael Mora

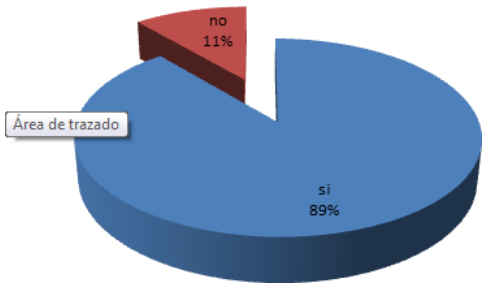

Grafico 5: Equipo del laboratorio

Elaborado por: Michael Mora

Análisis

El 90% del estudiante respondió que en su gran mayoría aprovechan los tiempos de uso de los laboratorios; es decir que el personal estudiantil aprovecha de manera eficiente el laboratorio

PREGUNTA 6 (sólo para personal de Tics)

¿La cantidad de desarrolladores es suficiente para cubrir la necesidad de mejoras en el ITB?

Cuadro 6: Cantidad de Desarrolladores

Alternativas	Muestra	Porcentaje
SI	6	60%
NO	4	40%
TOTAL	10	100%

Elaborado por: Michael Mora

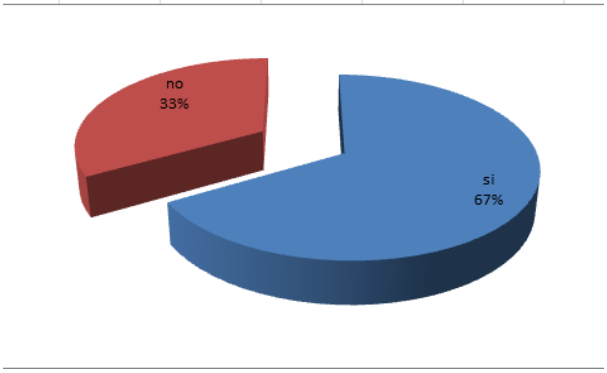

Grafico 6: Cantidad de desarrolladores

Elaborado por: Michael Mora

Análisis

El 67% del personal respondió que Si es suficiente el número de desarrolladores actual, mientras el 44% explican que es factible unir más personal a las filas de los desarrolladores; es decir que el personal que labora asegura existe suficientes desarrolladores en el área de tics ; aunque importante resaltar que si llegara a faltar algún desarrollador podría retrasar algún proyecto retrasaría las clases un día

PREGUNTA 7 (sólo para personal de Tics)

¿Se clasifica la gravedad del daño a los equipos, previo a la notificación de Tics?

Cuadro 7: Gravedad de daños

Alternativas	Muestra	Porcentaje
SI	9	100%
NO	0	0%
TOTAL	10	100%

Elaborado por: Michael Mora

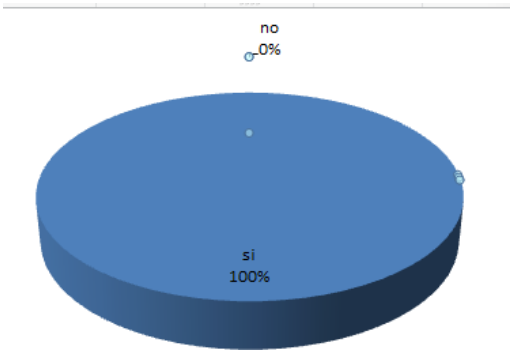

Grafico 7: Gravedad de daños

Elaborado por: Michael Mora

Análisis

El 100% del personal respondió que Si alguna daño se notifica en algún bien informático se procederá a clasificar el nivel de daño del mismo; es decir que el personal que labora asegura resolver cualquier imprevisto que se le presente a algún bien informático

PREGUNTA 8 (sólo para personal de Tics)

¿Usted identifica con facilidad el grado de daño del equipo averiado?

Cuadro 8: Equipo Averiado

Alternativas	Muestra	Porcentaje
SI	7	78%
NO	2	22%
TOTAL	10	100%

Elaborado por: Michael Mora

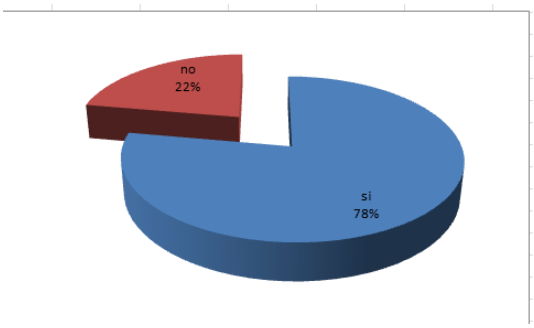

Grafico 8: Equipo Averiado

Elaborado por: Michael Mora

Análisis

El 78% del personal respondió que Si es suficiente el personal puede identificar después de un checkeo cualquier daño que tengan los equipos, mientras el 22% explican que algunos daños no son identificable a la primera revisión; es decir que el personal que labora asegura que la gran mayoría de daños pueden ser identificados y resueltos con facilidad

PREGUNTA 9

¿Cree usted que al realizar controles preventivos evitara posibles daños en el futuro?

Cuadro 9: Controles Preventivos

Alternativas	Muestra	Porcentaje
SI	9	100%
NO	0	0%
TOTAL	9	100%

Elaborado por: Michael Mora

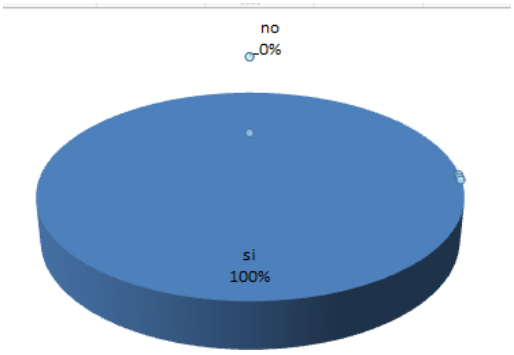

Grafico 9: Controles Preventivos

Elaborado por: Michael Mora

Análisis

El 100% del personal respondió que Si alguna daño puede ser evitado la mejor solución es utilizar un plan de controles preventivos; es decir que el personal que labora asegura prever cualquier imprevisto que se le presente a algún bien informático

PREGUNTA 10

¿Considera usted que con las sugerencias de un plan de mejoras puede contribuir en la forma de reaccionar ante algún imprevisto?

Cuadro 10: Plan de Mejoras

Alternativas	Muestra	Porcentaje
SI	6	60%
NO	3	30%
TOTAL	9	100%

Elaborado por: Michael Mora

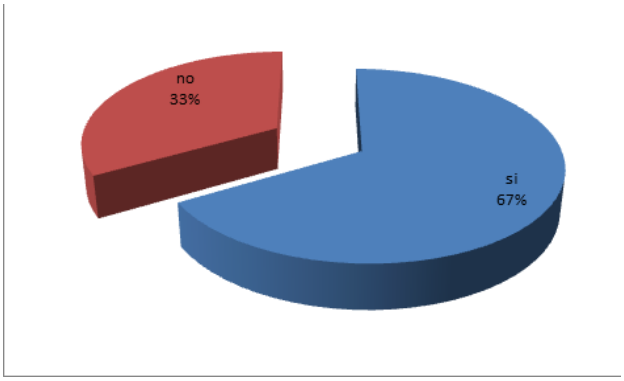

Grafico 9: Plan de mejoras

Elaborado por: Michael Mora

Análisis

El 67% del personal respondió que con un plan de mejoras renovado puede mejorar las posibilidades de solución a algún problema, mientras el 33% que el plan actual es bastante funcional por lo que no es necesario mejorarlo; es decir que el personal que labora asegura que la gran mayoría de daños pueden ser identificados y resueltos con facilidad

4.2. PLAN DE MEJORAS

4.2.1. SOLUCIÓN PROPUESTA Y PLAN DE CONTINGENCIAS

De acuerdo al análisis realizado, se presentan las sugerencias de los casos para combatir cada uno de los riesgos potenciales a los que se enfrenta el área de Tics Del Instituto Tecnológico Bolivariano.

El detalle de los planes de contingencia está en el Anexo 7.

4.2.2. RECOMENDACIONES CONTRA ACCESOS NO AUTORIZADOS

Frente a este riesgo potencial, es necesario implementar lo siguiente:

RECOMENDACIONES A NIVEL FÍSICO

- El servidor de archivos no debe ser accesible físicamente a cualquier Persona.
- Es conveniente que exista un espacio físico donde se ubique el Servidor, con acceso restringido al personal autorizado, y que cumpla con los requisitos adecuados para su funcionamiento, como temperatura ambiental adecuada, aislado del polvo y plagas dañinas.
- En este espacio, además de ubicar el servidor, se pueden ubicar los Elementos más sensibles de la red corporativa como el HUB/Switch y el servidor proxy.

RECOMENDACIONES A NIVEL LÓGICO

Habilitar un firewall que evite ingresos desde redes externas hacia la Red corporativa. Para la implementación del mismo presentamos las siguientes opciones:

La primera opción consta de configurar adecuadamente el firewall que viene incluido con el sistema operativo Linux Suse 8.0.

La segunda opción sería adquirir un hardware de seguridad que entre sus características tenga implementado un firewall

La recomendación de hardware incrementaría el costo de seguridad los cuales se verían justificados por la posible expansión de la empresa.

Instalar un sistema de detección de intrusos para monitorear los accesos o tentativas de accesos a la red corporativa.

La primera opción es un software de IDS instalado en el servidor proxy de la red. Este puede ser LIDS (Linux Intrusión Detection System), que es un parche del kernel de Linux que permite implementar funcionalidades de IDS al sistema operativo, y debido a ser open source, no tiene costo.

- Deshabilitar los servicios que no sean necesarios y luego de esto verificar los posibles puertos que se encuentren abiertos innecesariamente para proceder a cerrarlos. Esta información se encuentra detallada en la situación actual (capítulo 1).
- Concienciar a los usuarios de la red, se deberá concienciar a los usuarios de la red, acerca de una política mínima de seguridad, por ejemplo, evitar las claves fácilmente descifrables.
- Solo está permitido instalar en las computadoras el software requerido para el desarrollo de las actividades de la empresa, para esto se contará con un listado de dicho software, el cual deberá ser seleccionado por la Gerencia y jefes de área.
- Teniendo presente que la mayoría de los ataques informáticos no vienen de fuera, sino de dentro, según lo indican las estadísticas de penetración a las redes corporativas expuestas en el anexo D, un usuario interno podría capturar contraseñas con una herramienta sniffer.
- Para evitarlo, es conveniente que la red, en lugar de estar basada en un HUB, esté basada en conmutador (SWITCH).

  Eso evitará que todos los paquetes de información lleguen a todas las tarjetas de red. Usando una red conmutada puede evitar muchos intentos de espionaje de la información que circula por la red.

- Es recomendable agregar contraseña del BIOS a todos los equipos de

la red, para evitar vulnerabilidades de acceso dependientes de los Sistemas Operativos Instalados.

RECOMENDACIONES PARA PREVENIR FALLAS EN LOS EQUIPOS

- La primera opción será designar a uno o más empleados a que Dediquen un tiempo para el aprendizaje y formación, mediante la toma de un curso, para que ellos sean los encargados en brindar mantenimiento preventivo y correctivo a los equipos que posee la empresa.

  Como otra opción sugerimos el contratar los servicios de una empresa que de forma periódica realice mantenimiento preventivo a los equipos y correctivo si lo amerita la situación.

  Sea la decisión que sé que se escoja se sugiere que como mínimo se realice por lo menos una vez al año y llevar un control, de la vida útil de los diferentes dispositivos.

- Para evitar el caos que provocaría una avería en el servidor de archivos, o en uno de sus discos duros, plantéese la utilización de un cluster.
- Un sistema de alimentación sin interrupciones (UPS) es hoy en día Imprescindible, al menos para el servidor de archivos, el servidor proxy y el HUB/Switch.

- Al llevar un control de lo instalado mediante las listas de software se recomienda que todo nuevo software que se piense instalar sea probado en un computador que posea el software estándar para las actividades de la empresa con la finalidad de confirmar que este nuevo software no afectara a los otros ya instalados.
-

RECOMENDACIONES CONTRA EL ROBO DE DATOS Y FRAUDE

MEDIDAS PREVENTIVAS CONTRA EL ROBO DE DATOS

- Publicar la Política de Seguridad de la empresa.
- Promover el concepto de responsabilidad del empleado.
- Capacitar a los empleados para estar en alerta ante ladrones (y que vean la importancia del robo a la empresa)
- Entrevistar bien a los postulantes.
- Exigir certificado de antecedentes.
- Revisar bien sus referencias.
- Capacitar bien a los empleados nuevos en los procedimientos.
- Dar énfasis a las políticas de seguridad de la empresa.
- Mantener la puerta trasera cerrada.
- Mantener un ambiente de trabajo limpio y ordenado.
- Desarrollar buenos canales de comunicación con los empleados para resolver quejas.
- Capacitar a los empleados para que tengan una carrera profesional dentro de la empresa.
- El liderazgo - el jefe debe poner el ejemplo en seguir las normas.
- Ser duro con los empleados que roban, como ejemplo a los demás.

CÓMO PREVENIR ATAQUES DE INGENIERÍA SOCIAL

Para comprobar si se están realizando ataques de este tipo se recogerán estadísticas de incumplimiento de procedimientos. Por ejemplo, analizar el número de personas que han llamado a la empresa y que no se les ha entregado la información porque no proporcionaban todos los datos de identificación solicitados. Poder reconocer ciertas señas típicas de una acción de esta naturaleza, como son rehusarse a entregar información de contacto, tener mucho apuro, referenciar a una persona importante, intimidación o

requerimiento de información olvidada, por enumerar las más comunes, es claramente otra manera de estar alertas. De cualquier forma, en la actualidad, es vital educar, capacitar, sensibilizar sobre las políticas y procedimientos definidos y que son relativos a este tema.

Una forma de defensa contra estos ataques es conocer los conceptos básicos que pueden ser utilizados contra una persona o la compañía a la que pertenece y que abren brechas para conseguir datos. Con este conocimiento se debe adoptar una actitud proactiva que alerte y concienciar a los empleados que avisen de cualquier pregunta o actitud sospechosa. Eso sí, las políticas de seguridad deben ser realistas con reglas concisas y concretas que se puedan cumplir.

4 PLANES DE CONTINGENCIARECOMENDACIONES REALIZAR LA ACTUALIZACIONES DE PARCHES DE SEGURIDAD

Como complemento a las sugerencias anteriores, es recomendable estar al día con la instalación de los diferentes parches de seguridad para el software de la empresa.

Debido a que la mayoría de equipos funcionan bajo ambiente Microsoft, es conveniente instalar un servidor SUS, que realice las funciones de actualización de los parches de seguridad de los sistemas operativos Windows instalados en la red. Para esto se configuraría el servidor central para que descargue las actualizaciones y las almacene en disco duro, luego los clientes (estaciones de la red) automáticamente realizarían la actualización conectándose a este servidor. Este proceso se debería ejecutar en horarios que no afecten el desempeño de la red.

También se deben descargar los parches de seguridad para las demás aplicaciones que se utilizan en la empresa, como los productos Oracle, de manera que sé este al día con las correcciones de las vulnerabilidades existentes.

Las recomendaciones de lo que debe realizarse en el caso de presentarse una contingencia como fuego, terremoto o un robo físico, se las podrá encontrar a continuación en el plan de contingencias.

4.1.2 ASPECTOS GENERALES DE LA SEGURIDAD DE LA INFORMACIÓN.

La Seguridad Física La seguridad física garantiza la integridad de los activos humanos, lógicos y materiales de un sistema de información de datos. Si se entiende la contingencia o proximidad de un daño como la definición de Riesgo de Fallo, local o general, tres serían las medidas a preparar para ser utilizadas en relación a la cronología del fallo.

El nivel adecuado de seguridad física, o grado de seguridad, es un conjunto de acciones utilizadas para evitar el fallo o, en su caso, aminorar las consecuencias que de el se puedan derivar. Es un concepto aplicable a cualquier actividad, no sólo a la informática, en la que las personas hagan uso particular o profesional de entornos físicos.

- Ubicación del edificio.
- Ubicación del Centro de Procesamiento de Datos dentro del edificio.
- Compartimentación.
- Elementos de la construcción.
- Potencia eléctrica.
- Sistemas contra Incendios.
- Control de accesos.
- Selección de personal.
- Seguridad de los medios.
- Medidas de protección.

• Duplicación de medios.

Durante Se debe de ejecutar un plan de contingencia adecuado. En general, cualquier desastre es cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el normal proceso de una empresa. La probabilidad de que ocurra un desastre es muy baja, aunque se diera, el impacto podría ser tan grande que resultaría fatal para la organización. Por otra parte, no es corriente que un negocio responda por sí mismo ante un acontecimiento como el que se comenta, se deduce la necesidad de contar con los medios necesarios para afrontarlo. Estos medios quedan definidos en el Plan de Recuperación de Desastres que junto con el Centro Alternativo de Proceso de Datos, constituye el plan de contingencia que coordina las necesidades del negocio y las operaciones de recuperación del mismo. Son puntos imprescindibles del plan de contingencia

• Realizar un análisis de riesgos de sistemas críticos que determine la tolerancia de los sistemas

• Establecer un periodo crítico de recuperación, en la cual los procesos debe de ser reanudados antes de sufrir pérdidas significativas o irrecuperables.

• Realizar un Análisis de Aplicaciones Críticas por que se establecerán las prioridades del proceso.

• Determinar las prioridades del proceso, por días del año, que indiquen cuales son las aplicaciones y sistemas críticos en el momento de ocurrir el desastre y el orden de proceso correcto. Plan de Contingencia de los Sistemas de Información 10 Instituto Nacional de Estadística e Informática

• Establecer objetivos de recuperación que determinen el período de tiempo (horas, días, semanas) entre la declaración de desastre y el momento en el que el centro alternativo puede procesar las aplicaciones críticas.

• Designar entre los distintos tipos existentes, un Centro Alternativo de Proceso de Datos.

• Asegurar la capacidad de las comunicaciones.

• Asegurar la capacidad de los servidores back-up. 5.1.3 Después Los contratos de seguros vienen a compensar, en mayor o menor medida las pérdidas, gastos o responsabilidades que se puedan derivar para el centro de proceso de datos una vez detectado y corregido el fallo. De la gama de seguros existentes, se pueden indicar los siguientes:

• **Centros de proceso y equipamiento**: se contrata la cobertura sobre el daño físico en el CPD (Centro de Procesamiento de Datos) y el equipo contenido

• **Reconstrucción** de medios de software: cubre el daño producido sobre medio software tanto los que son de propiedad del tomador de seguro como aquellos que constituyen su responsabilidad.

• **Gastos extra:** cubre los gastos extra que derivan de la continuidad de las operaciones tras un desastre o daño en el centro de proceso de datos. Es suficiente para compensar los costos de ejecución del plan de contingencia.

• **Interrupción del negocio**: cubre las pérdidas de beneficios netos causadas por las caídas de los medios informáticos o por la suspensión de las operaciones.

• **Documentos y registros valiosos:** Se contrata para obtener una compensación en el valor metálico real por la pérdida o daño físico sobre documentos y registros valiosos no amparados por el seguro de reconstrucción de medio software.

• **Errores y omisiones**: proporciona protección legal ante la responsabilidad en que pudiera incurrir un profesional que cometiera un acto, error u omisión que ocasione una pérdida financiera a un cliente.

• **Cobertura de fidelidad**: cubre las pérdidas derivadas de actos deshonestos o fraudulentos cometidos por empleados.

• **Transporte de medios:** proporciona cobertura ante pérdidas o daños a los medios transportados.

• **Contratos con proveedores y de mantenimiento:** proveedores o fabricantes que aseguren la existencia de repuestos y consumibles, así como garantías de fabricación.

Seguridad Integral de la Información La función del procesamiento de datos es un servicio de toda la institución, que apoya no sólo a los sistemas de información administrativa sino también a las operaciones funcionales. La Seguridad un aspecto de mucha importancia en la correcta Administración Informática, lo es también de toda la Institución. Las medidas de seguridad están basadas en la definición de controles físicos, funciones, procedimientos y programas que conlleven no sólo a la protección de la integridad de los datos, sino también a la seguridad física de los equipos y de los ambientes en que éstos se encuentren. En relación a la seguridad misma de la información, estas medidas han de tenerse en cuenta para evitar la pérdida o modificación de los datos, información o software inclusive, por personas no autorizadas, para lo cual se deben tomar en cuenta una serie de medidas, entre las cuales figurarán el asignar números de identificación y contraseñas a los usuarios.

4.1.3 RECOMENDACIONES CONTRA ACCESOS NO AUTORIZADOS

Frente a este riesgo potencial, es necesario implementar lo siguiente:

RECOMENDACIONES A NIVEL FÍSICO

- El servidor de archivos no debe ser accesible físicamente a cualquier Persona.

- Es conveniente que exista un espacio físico donde se ubique el Servidor, con acceso restringido al personal autorizado, y que cumpla con los requisitos adecuados para su funcionamiento, como temperatura ambiental adecuada, aislado del polvo y plagas dañinas.
- En este espacio, además de ubicar el servidor, se pueden ubicar los Elementos más sensibles de la red corporativa como el HUB/Switch y el servidor proxy.

RECOMENDACIONES A NIVEL LÓGICO

- Habilitar un firewall que evite ingresos desde redes externas hacia la Red corporativa. Para la implementación del mismo presentamos las siguientes opciones:

La primera opción consta de configurar adecuadamente el firewall que viene incluido con el sistema operativo Linux Suse 8.0.

La segunda opción sería adquirir un hardware de seguridad que entre sus características tenga implementado un firewall

La recomendación de hardware incrementaría los costó de seguridad los cuales se verían justificados por la posible expansión de la empresa.

- Instalar un sistema de detección de intrusos para monitorear los Accesos o tentativas de accesos a la red corporativa para esto presentamos a continuación dos opciones:

La primera opción es un software de IDS instalado en el servidor proxy de la red. Este puede ser **LIDS** (Linux Intrusión Detection System), que es un parche del kernel de Linux que permite implementar funcionalidades de IDS al sistema operativo, y debido a ser open source, no tiene costo.

- Deshabilitar los servicios que no sean necesarios y luego de esto Verificar los posibles puertos que se encuentren abiertos innecesariamente para proceder a cerrarlos. Esta información se encuentra detallada en la situación actual (capítulo 1).

- Concienciar a los usuarios de la red, se deberá concienciar a los Usuarios de la red, acerca de una política mínima de seguridad, por ejemplo, evitar las claves fácilmente descifrables.

- Solo está permitido instalar en las computadoras el software Requerido para el desarrollo de las actividades de la empresa, para esto se contará con un listado de dicho software, el cual deberá ser seleccionado por la Gerencia y jefes de área.

- Teniendo presente que la mayoría de los ataques informáticos no Vienen de fuera, sino de dentro, según lo indican las estadísticas de penetración a las redes corporativas expuestas en el anexo D, un usuario interno podría capturar contraseñas con una herramienta sniffer.

  Para evitarlo, es conveniente que la red, en lugar de estar basada en un HUB, esté basada en conmutador (SWITCH).

  Eso evitará que todos los paquetes de información lleguen a todas las tarjetas de red. Usando una red conmutada puede evitar muchos intentos de espionaje de la información que circula por la red.

- Es recomendable agregar contraseña del BIOS a todos los equipos de la red, para evitar vulnerabilidades de acceso dependientes de los Sistemas

  Operativos Instalados.

4.1.4 RECOMENDACIONES PARA PREVENIR FALLAS EN LOS EQUIPOS

- La primera opción será designar a uno o más empleados a que Dediquen un tiempo para el aprendizaje y formación, mediante la toma de un curso, para que ellos sean los encargados en brindar mantenimiento preventivo y correctivo a los equipos que posee la empresa.

  Como otra opción sugerimos el contratar los servicios de una empresa que de forma periódica realice mantenimiento preventivo a los equipos y correctivo si lo amerita la situación.

  Sea la decisión que sé que se escoja se sugiere que como mínimo se realice por lo menos una vez al año y llevar un control, de la vida útil de los diferentes dispositivos.

- Para evitar el caos que provocaría una avería en el servidor de archivos, o en uno de sus discos duros, plantéese la utilización de un cluster.
- Un sistema de alimentación sin interrupciones (UPS) es hoy en día Imprescindible, al menos para el servidor de archivos, el servidor proxy y el HUB/Switch.

  - Al llevar un control de lo instalado mediante las listas de software se recomienda que todo nuevo software que se piense instalar sea probado en un computador que posea el software estándar para las actividades de la empresa con la finalidad de confirmar que este nuevo software no afectara a los otros ya instalados.

4.1.5 RECOMENDACIONES CONTRA EL ROBO DE DATOS Y FRAUDE

MEDIDAS PREVENTIVAS CONTRA EL ROBO DE DATOS

- Publicar la Política de Seguridad de la empresa.
- Promover el concepto de responsabilidad del empleado.
- Capacitar a los empleados para estar en alerta ante ladrones (y que vean la importancia del robo a la empresa)
- Entrevistar bien a los postulantes.
- Exigir certificado de antecedentes.
- Revisar bien sus referencias.
- Capacitar bien a los empleados nuevos en los procedimientos.
- Dar énfasis a las políticas de seguridad de la empresa.
- Mantener la puerta trasera cerrada.
- Mantener un ambiente de trabajo limpio y ordenado.
- Desarrollar buenos canales de comunicación con los empleados para resolver quejas.
- Capacitar a los empleados para que tengan una carrera profesional dentro de la empresa.
- El liderazgo - el jefe debe poner el ejemplo en seguir las normas.
- Ser duro con los empleados que roban, como ejemplo a los demás.

CÓMO PREVENIR ATAQUES DE INGENIERÍA SOCIAL

Para comprobar si se están realizando ataques de este tipo se recogerán estadísticas de incumplimiento de procedimientos. Por ejemplo, analizar el número de personas que han llamado a la empresa y que no se les ha entregado la información porque no proporcionaban todos los datos de identificación solicitados. Poder reconocer ciertas señas típicas de una acción de esta naturaleza, como son rehusarse a entregar información de contacto, tener mucho apuro, referenciar a una persona importante, intimidación o

requerimiento de información olvidada, por enumerar las más comunes, es claramente otra manera de estar alertas. De cualquier forma, en la actualidad, es vital educar, capacitar, sensibilizar sobre las políticas y procedimientos definidos y que son relativos a este tema.

Una forma de defensa contra estos ataques es conocer los conceptos básicos que pueden ser utilizados contra una persona o la compañía a la que pertenece y que abren brechas para conseguir datos. Con este conocimiento se debe adoptar una actitud proactiva que alerte y concienciar a los empleados que avisen de cualquier pregunta o actitud sospechosa. Eso sí, las políticas de seguridad deben ser realistas con reglas concisas y concretas que se puedan cumplir.

4.1.6 PROTECCIÓN PARA CORREO CORPORATIVO

Se recomienda el uso de una herramienta que permita implementar infraestructura de clave pública para proteger la comunicación por correo electrónico que implique el envío de información confidencial.

Unas de las herramientas recomendadas para este propósito es el Lotus Notes Domino para Windows.

4.2 CONCLUSIONES Y RECOMENDACIONES

4.2.1 Conclusiones

La investigación ha listado de estudiar el mejoramiento del área de tics por medio de los planes de contingencia existentes con el fin de poder sugerir posibles soluciones herramienta tecnológica

Una vez obtenido el análisis de la información que suministro la aplicación de la encuesta a los docentes e involucrados del área de tics sobre los planes de contingencia y la importancia de colaborar entre sí para prevenir algún imprevisto que pueda surgir

4.2.2 Recomendaciones

- Mejorar el proceso de investigación, ampliando la variedad de instrumentos para la recolección de la información, e incluir a los docentes con, el fin de tener un mayor área cubierta para prevenir y corregir daños
  - Todas las acciones emprendidas por el gerente de tics debe centrarse en un liderazgo eficaz, el cual se concibe como, la influencia sobre las personas para que trabajen con aclamación en la consecución de objetivos en pro del bien común.
  - Todas las acciones emprendidas por el gerente educativo debe centrarse en un liderazgo eficaz, el cual se concibe como, la influencia sobre las personas para que trabajen con aclamación en la consecución de objetivos en pro del bien común.

BIBLIOGRAFIA

Centro Nacional ECU911-Institucion . (2013). Recuperado el 14 de Junio de 2015, de http://www.ecu911.gob.ec/la-institucion/

Administracion Web. (2014). Recuperado el 25 de Septiembre de 2015, de http://simpl202.com/servicios_web/administracion-de-paginas-web/

Antonio, O. S. (2012). *Aplicaciones web*. Recuperado el 19 de Junio de 2015, de http://sedici.unlp.edu.ar/handle/10915/2475

Brouyere, J. D. (2014). *Investigación Exploratoria, Descriptiva, Correlacional y Explicativa.* http://datateca.unad.edu.co/contenidos/100104/100104_EXE/leccin_6_investigacin_exploratoria_descriptiva_correlacional_y_explicativa.html.

Brouyere, J. D. (2014). *Investigación Exploratoria, Descriptiva, Correlacional y Explicativa.* http://datateca.unad.edu.co/contenidos/100104/100104_EXE/leccin_6_investigacin_exploratoria_descriptiva_correlacional_y_explicativa.html.

Brouyere, J. D. (2014). *Investigación Exploratoria, Descriptiva, Correlacional y Explicativa.* http://datateca.unad.edu.co/contenidos/100104/100104_EXE/leccin_6_investigacin_exploratoria_descriptiva_correlacional_y_explicativa.html.

Camazón, J. n. (2012). *Sistemas Operativos Monopuesto.*

CARDONA, E. (2011). *Auditoria de sistemas de información.* http://www.gerencie.com/auditoria-de-sistemas-de-informacion.html.

Castro, i. L. (2014). *Proyecto de Tesis*. Recuperado el 16 de Junio de 2015, de http://www.academia.edu/6870973/PROYECTO_DE_TESIS

castro, s. (2013). *SOPORTE TECNICO.* http://soporte-tecni.blogspot.com/2013/03/soporte-tecnico.html.

Cortez, D. (2012). Significado de Contingencia.

Ecu911, S. I. (6 de Febrero de 2012). *Inauguracion del Sistema Ecu911*. Recuperado el 20 de Septiembre de 2015, de Inauguracion del Sistema Ecu911: http://www.presidencia.gob.ec/wp-content/uploads/downloads/2012/10/2012-02-06-Inauguracion-del-Sistema-Integrado-ECU-911.pdf

Ecu-911, S. I. (2015). *Centro de Seguridad*. Recuperado el 17 de Junio de 2015, de http://www.ecu911.gob.ecwww.seguridad.gob.ecwww.nuestraseguridad.gob.ec/es

El Universo. (06 de Febrero de 2012). *Servicio Integrado Seguridad*. Recuperado el 17 de Junio de 2015, de http://www.eluniverso.com/2012/02/06/1/1422/servicio-integrado-seguridad-ecu-911-entro-funcionamiento.html

Embajada, E. (2011). *Modelo de Relacionamiento en Materia de Seguridad*. Recuperado el 20 de Septiembre de 2015, de http://www.embassyecuador.eu/site/images/descargas/seguridad-ciudadana.pdf

Franco, Y. (31 de Mayo de 2011). *Tesis de Investigacion*. Recuperado el 16 de Junio de 2015, de http://tesisdeinvestig.blogspot.com/2011/05/tipos-de-investigacion.html

Galindo, M. J. (2011). *Escaneando la Informática* .

ICE. (2011). Nuevas Trcnologias. *RevistaICE*, 57.

J., M. F. (2012). *Sitios Web*. Recuperado el 19 de Junio de 2015, de http://eprints.rclis.org/8998/

Jeremias. (2011). *Concurso anual de investigacion de la OLACEF 2011 denominado "Audirorias de gestion a las tecnologias de informacion y comunicaciones".* El Salvador: Concurso de investigacion.

LACCEI. (22 de Julio de 2014). *Aplicación de la Metodologia ICONIX*. Recuperado el 15 de Agosto de 2015, de http://www.laccei.org/LACCEI2014-Guayaquil/RefereedPapers/RP246.pdf

Malhotra, N. K. (2008). *Investigacion de mercados.* Prentice Hall.

Margalef, J. C. (2011). *Dinalte*. Recuperado el 18 de Junio de 2015, de http://dialnet.unirioja.es/servlet/articulo?codigo=12623

Martinez, F. A. (2013). *Soporte Técnico Presencial.* http://soportetecnicopresencialcecyte3.blogspot.com/.

Martinez, V. (2010). Agendas Virtuales. *Comillas*, 326.

Mercedes Alba, C. O. (2014). Virtualidad. *Revista Cientifica de la Escuela de Postgrados de Colombia*, 150.

Mora, S. J. (2011). *Programación en Internet: clientes Web.*

Morales, E. (2012). *Los servicios informaticos y su importancia.* http://www.mikogo.es/2011/03/01/servicios-informaticos-importancia/.

O'Higgins, B. (2012). *Definición e implementación.* http://www.convivenciaescolar.cl/index2.php?id_portal=50&id_seccion=4020&id_contenido=17983.

Osti, M. V. (2011). *La Web*. Recuperado el 19 de Junio de 2015, de http://dialnet.unirioja.es/servlet/libro?codigo=321909

Padilla Castro, L. (2014). *Proyecto de Tesis*. Recuperado el 16 de Junio de 2015, de http://www.academia.edu/6870973/PROYECTO_DE_TESIS

Parra Galvis, A. (2012). *Auditoria de sistemas de información.* http://www.gerencie.com/auditoria-de-sistemas-de-informacion.html.

Peña, J. G. (2010). *Dialnet*. Recuperado el 20 de Junio de 2015, de http://dialnet.unirioja.es/servlet/libro?codigo=316434

Ramírez, I. A. (2011). *Conceptos Básicos de Internet.* http://conceptosbasicosdeinternetarr.blogspot.com/2011/07/internet-definicion-e-historia.html.

Ramirez, L. A. (Agosto de 2014). *Fundamentos de Administracion* . Recuperado el 20 de Septiembre de 2015, de http://www.uv.mx/personal/alsalas/files/2014/09/INTRODUCCION-A-LA-ADMINISTRACION.pdf

Reino, U. (18 de Septiembre de 2014). *Indra*. Recuperado el 27 de Septiembre de 2015, de 18 septiembre 2014 (Reino Unido

Salasar, J. B. (2012). *Modelo Para Seguridad de la Información en TIC.* Concepcion,Chile.

SECOM. (06 de Febrero de 2015). *El Ciudadano*. Obtenido de http://www.laciudadana.gob.ec/index.php/template/radio-ciudadana-historia/item/5687-ecu-911-cumple-3-anos-en-ecuador.html

Senplades. (2014). *Buen Vivir Plan Nacional 2013-2017*. Recuperado el 15 de Junio de 2015, de http://www.buenvivir.gob.ec/objetivo-7.-garantizar-los-derechos-de-la-naturaleza-y-promover-la-sostenibilidad-ambiental-territorial-y-global

Senplades. (2014). *BuenVivir Plan Nacional 2013-2017*. Recuperado el 15 de Junio de 2015, de

http://documentos.senplades.gob.ec/Plan%20Nacional%20Buen%20Vivir%202013-2017.pdf

Sierra, M. (2013). *Qué es un servidor y cuáles son los principales tipos de servidores (proxy,dns, web,ftp,pop3 y smtp, dhcp...).* http://aprenderaprogramar.com/index.php?option=com_content&view=article&id=542:que-es-un-servidor-y-cuales-son-los-principales-tipos-de-servidores-proxydns-webftppop3-y-smtp-dhcp&catid=57:herramientas-informaticas&Itemid=179.

Tancara, G. C. (Diciembre de 2013). *Guia para la formulacion proyectos de invetigacion* . Recuperado el 16 de Junio de 2015, de http://www.dicytuap.edu.bo/guias/Guia_formulacion_Proyectos_Investigacion.pdf

Tancara, i. G. (Diciembre de 2013). *Guia para la Formulacion de Proyecos de Investigacion* . Recuperado el 16 de Junio de 2015, de http://www.dicytuap.edu.bo/guias/Guia_formulacion_Proyectos_Investigacion.pdf

Teckelino., T. (2011). *ELABORACIÓN DE UN PLAN DECONTINGENCIA BASADO EN UNANÁLISIS DE RIESGO.* http://es.scribd.com/doc/43714047/Plan-de-contingencia-sistemas-informaticos#scribd.

Toro, M. d. (2010). *Auditoria de gestion de las tics para la empresa dipac utilizando cobit.* quito: Tesis.

Umaginga, L. (2010). *Aplicaciones Virtuales*. Recuperado el 20 de Junio de 2015, de http://upcommons.upc.edu/handle/2099.1/23618

Villoria, R. M. (2012). *APLICACIONES WEB 2.0 - Google docs.*

ANEXO No. 1

Contingencias y recuperación de desastres

Respaldo de la información

El respaldo de la información que tenemos almacenada en el disco duro de la computadora de la oficina o en el servidor de la red, es el último recurso en caso de que ocurra alguna de las siguientes situaciones típicas:

- Fallas del disco duro
- Interrupciones de energía
- Energía no regulada
- Errores del personal de operación
- Errores de programación (sobre todo al modificar alguna aplicación, Incompatibilidades)
- Inundación, incendio, desastre
- Problemas climatológicos
- Infecciones con virus
- Robos

Año: 2015

ANEXO No. 2

Anexo N° 2

Obtención y almacenamiento de los respaldos de información (BACKUPS)

Se obtendrán copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la Institución. Para lo cual se debe contar con:

- Backups del Sistema Operativo.
- Backups del Software Base - Paquetes y/o Lenguajes de Programación.
- Backups de Productos Desarrollados (Considerando tanto los programas fuentes, como los programas objetos correspondientes)
- Backups de los Datos (Bases de Datos, Índices, y todo archivo necesario para la correcta ejecución de los Productos Desarrollados)

Backups del Hardware, mediante convenio con otra Institución que tenga equipos similares o mayores y que brinden la seguridad de poder continuar con las actividades para ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido. Este tipo de convenios debe tener tanto las consideraciones de equipamiento como ambiente y facilidades de trabajo.

Año: 2010

ANEXO No. 3

Encuesta

1. ¿En su empresa existe un sistema computarizado, que le permita el control de su mercadería en el área de tics?

Si ☐

No ☐

Si 7 no 3

2. ¿Cree usted que se tiene suficientes usuarios con códigos de acceso remoto?

Si ☐

No ☐

4. ¿En el departamento de bodega se encuentran todos los productos clasificados y contabilizados?

Si ☐

No ☐

5. ¿Al momento del usuario tiene un problema en el sistema puede ser ayudado ?

Si ☐

No ☐

6. ¿Realizan el inventario físico de productos dentro del tiempo estimado de labores?

Si ☐

No ☐

7. ¿La cantidad de desarrolladores abarca la necesidad de mejoras en el departamento de desarrollo?

Si ☐

No ☐

8. ¿Se clasifican la gravedad de daños en algún equipo previo a su reparación?

Si ☐

No ☐

9. ¿Usted identifica con facilidad la cantidad de equipo averiado?

Si ☐

No ☐

10. ¿Cree usted que al realizar controles preventivos evitara posibles daños en el futuro?

Si ☐

No ☐

11. ¿Considera usted que con la sugerencias de un plan de mejoras puede contribuir en la forma de reaccionar ante algún imprevisto?

Si ☐

No ☐

Año: 2014

Fuente:

ANEXO No. 4

Entrevista

1) ¿Cuál es la causa principal, de que desean incorporar a su plan de contingencias?

_____

_____

2) ¿Cómo controla la entrada y salida de la mercadería que se compra para la venta para el uso de los equipos?

_____

_____

3) ¿Qué tiempo tarda en realizar el mantenimiento a los servidores ?

_____

_____

4) ¿Dentro de la mercadería existen productos que no graban IVA?

_____

_____

5) ¿El personal que labora en su empresa se encuentra capacitado para administrar el sistema?

_____

_____

6) ¿Cómo ejecuta el proceso de facturación?

_____

_____

7) ¿Cómo comprueba la existencia o faltante de mercadería?

_____

_____

8) ¿Cree usted que los planes de contingencia deben ser mejorados?

_____

_____

9) ¿Conoce usted con certeza la cantidad de materiales y productos que necesiten mantenimiento?

_____

_____

10) ¿Considera usted que la actual plan de contingencia esta estructurando ante cualquier fallo?

_____

_____

Año: 2015

Fuente:

ANEXO No. 5

Anexo N° 5

Lcda. Tatiana Tapia Bastidas ,Mae, PhD	Directora de Tics
Tnlgo. Nelson Villacres	Jefe de soporte Técnico
Ing. Daniel Navarrete	Soporte Aplicativo y Hardware
Ing. Andrea Aquino	Soporte Aplicativo y Hardware
Ing. Soraya Gallegos	Jefe de Programación
Ing. Juan José Urgirles	Analista Programador
Anl. Olga Castillo	Analista Programador
Ing. Rene Cardona	Programador web
Tnlgo. Adriana Peñafiel	Diseñadora Grafica

Año: 2015

Fuente:

ANEXO No. 6

ANTECEDENTES HISTORICOS

Creación del área de tics

El área de tics del Instituto Superior Tecnológico Bolivariano de Tecnología fue formalmente creado en junio del 2012, anteriormente se tenía una jefatura de sistemas que proponía soluciones de programación y las implementaba en todo el tecnológico, esta jefatura no se involucraba con la atención a los requerimientos tecnológicos los cuales eran solucionados directamente por el señor Rector el cual tiene formación de Licenciado en Sistemas de Información; sin embargo y debido al inusual incremento de estudiantes y por ende del aumento de los servicios sistematizados, hubo que recurrir a la implementación de un área de tics que resuelva dicha sistematización.

Referencia

n

http://www.itb.edu.ec/antecedentes/

ANEXO No. 7

Instituto Tecnológico Bolivariano Registro de CONESUP 09-030	**PROCEDIMIENTO** **CONTINGENCIA PARCHES EN APLICACIONES WEB**		**Pagina 1/3**
Código: SIS-001-2015	**Revisión Ant.: N/A**	**Vigencia: Nov 2015**	

Objetivo

Para los responsables de decisiones TI y los profesionales de la tecnología nuevos en la gestión de parches de seguridad, información útil que toda empresa debería entender sobre cómo Microsoft aborda las vulnerabilidades y actualizaciones de seguridad, además de información concisa sobre procesos, herramientas, técnicas y recursos para realizar de forma eficaz la gestión de parches de seguridad

Alcance

El coste operacional de un día de inactividad puede calcularse, pero ¿qué ocurre si la información que otros han encomendado a su empresa es puesta en peligro públicamente?

Una brecha de seguridad corporativa y la consiguiente pérdida de credibilidad (ante los clientes, los partners y el gobierno) pueden arriesgar la propia naturaleza de la empresa. Las empresas que no realizan una gestión proactiva de los parches de seguridad como parte de su estrategia de seguridad TI lo hacen por su cuenta y riesgo.

Documentos de referencia

- Manual de contingencia en aplicaciones web

Responsables

Departamento de Sistemas es responsable de la oportuna solución a las diferentes eventualidades que se presenten por falla de los parches en aplicaciones web.

Definiciones

Ninguna

Desarrollo de Procedimiento

PASO I: INFORMACIÓN ESENCIAL

1. Introducción a la Gestión de Parches de Seguridad

Trata varios problemas de seguridad de la industria del software y el impacto resultante que pueden tener sobre una empresa, introduce términos clave de uso frecuente en esta guía e identifica algunas vulnerabilidades de seguridad comunes, abusos históricos y las lecciones que se derivan de ellos.

2. Preparación para la Gestión de Parches

El paso 2 presenta los costes empresariales de omitir la gestión de parches y los pasos que debe seguir una empresa para prepararse satisfactoriamente para la gestión proactiva de parches. También identifica las responsabilidades clave necesarias durante el ciclo de vida de la gestión de parches.

3. Entender la Gestión de Parches de Seguridad

Este paso discute un proceso racionalizado de gestión de parches de seguridad y define los problemas, los conceptos clave y las prácticas recomendadas que todo profesional implicado en la gestión de parches debería entender. Este proceso racionalizado sirve también como base estructural para las técnicas y procesos prescriptivos presentados en la Parte II. Si va a leer la Parte II, no necesita leer este capítulo.

4. Herramientas y Tecnologías

Presenta las tecnologías de evaluación e implantación de parches de Microsoft, compara los costes y capacidades de cada una y proporciona orientación para ayudar a una empresa a decidir qué infraestructura de distribución de parches es apropiada para ella.

Apéndice A: Herramientas y Recursos de Terceros

Reúne una lista de algunos de los recursos y herramientas de terceras partes disponibles para ayudar en la gestión de parches de seguridad.

Registro

El registro es periódico dependiendo de la duración predeterminada del parche

Modificaciones o cambios

Fecha anterior	**Cambios o modificaciones**	**Fecha del cambio**
n/a	Creación del procedimiento	05/11/2015
Elaborado por: **Nombre: M.Mora** **Cargo:** **Fecha:**	**Revisado por:** **Nombre: T. Tapia** **Cargo: Dir.Sistemas** **Fecha:**	**Aprobado por:** **Nombre : R. Tolozano** **Cargo: Rector** **Fecha:**
Firma	**Firma**	**Firma**

Plan de contingencia para:

<table>
<tr><td rowspan="2">  </td><td colspan="2">PROCEDIMIENTO</td><td rowspan="2">Pagina 1/5</td></tr>
<tr><td colspan="2">CONTINGENCIA PARCHES EN ACCESO REMOTO SEGURO</td></tr>
<tr><td>Código: SIS-002-2015</td><td>Revisión Ant.: N/A</td><td>Vigencia: Nov 2015</td><td></td></tr>
</table>

Objetivo

El teletrabajo está integrado por dos áreas: el acceso remoto, es decir, la posibilidad de que las personas trabajen desde su casa; y la seguridad general de las redes.

Sin éstas, es muy complicado que una iniciativa de este tipo funcione de forma óptima y el de la seguridad es un gran punto en el cual nuestra empresa puede añadir gran valor para el futuro: la conexión segura.

Alcance

El trabajo a distancia o teletrabajo es una estrategia que sirve a las empresas para mantener la productividad de sus operaciones (dentro de ambientes seguros), en situaciones de contingencia como las que vivieron en México y Argentina debido a la influenza; pero, no solo.

El teletrabajo es una necesidad creciente de nuestras ciudades. En la actualidad muchos tipos de trabajo son perfectamente posibles de realizar desde los hogares. La gente ya no tiene que estar presente en las oficinas.

El acceso remoto es una tendencia en crecimiento. Pero ¿cómo hacerlo y al mismo tiempo defender los intereses de las compañías?, ¿cómo hacer que no se exponga la información confidencial?

Documentos de referencia

- Manual de acceso remoto seguro

Responsables

Departamento de Sistemas es responsable de la oportuna solución a las diferentes eventualidades que se presenten por falla del acceso remoto seguro más explícitamente es el Administrador de redes.

Definiciones

Ninguna

Desarrollo de Procedimiento

Servicios de Escritorio Remoto

Si los llamamos en inglés (Terminal Services) ya le será familiar a más de uno... Están recomendados para los servicios de aplicaciones en red, cuando se dispone de conectividad permanente y se destina a aplicaciones ligeras "en web". Como ventajas, la primera de ellas es que se trata de una tecnología madura, y sin ser menos importante, no hay datos en el puesto de trabajo cliente.

En el apartado de limitaciones, esta tecnología exige un esfuerzo de implantación elevado, no provee imagen del desktop de usuario y presenta un escaso soporte multimedia.

La tecnología Microsoft relacionada con esta opción se centra en los Microsoft Terminal Services, presentes en Windows Server desde hace varias generaciones, y ahora renombrados como Remote Desktop Services en Windows Server 2008 R2, en el que se han conseguido muchísimas mejoras de rendimiento en la experiencia del usuario, compatibilidad con Windows Installer RDS, y administración de la caché de los perfiles de usuarios roaming. También se integra con Hyper-V para brindar RemoteApp y RemoteDesktop a las máquinas virtuales, y el Remote Desktop Client 7.0 soporta Aero en las sesiones de Windows 7 y Windows Server 2008 R2.

Acceso seguro a aplicaciones remotas

Los productos de seguridad del perímetro y de acceso de Forefront, Internet Security and Acceleration (ISA) Server 2006 e Intelligent Application Gateway (IAG) 2007, proporcionan protección del perímetro de la red, así como acceso centrado en aplicaciones y basado en directivas a la infraestructura de TI corporativa, que incluye acceso remoto seguro, seguridad de las sucursales y protección de acceso a Internet.

Concretamente (y abundamos en detalles quizá por ser la menos conocida) Microsoft Intelligent Application Gateway (IAG) es una solución que permite el acceso a las aplicaciones y recursos corporativos desde cualquier parte manteniendo a los usuarios protegidos y productivos. Los usuarios pueden acceder desde su casa a todo lo que podrían acceder desde la empresa y de una manera sencilla y segura. IAG es un producto que combina el acceso a la red privada virtual basado en el protocolo SSL (Secure Socket Layer) y el firewall para aplicaciones Web obtenido tras la adquisición de Whale Communications en julio de 2006, con nuestra solución Microsoft Internet Security and Acceleration Server (ISA Server).

Virtual Desktop Infrastructure (VDI)

Con VDI centralizamos el almacenamiento y la ejecución de los puestos de trabajo (SO, aplicaciones, datos) en máquinas virtuales en el datacenter, presentando la interfaz gráfica usando un protocolo de acceso remoto (como RDP) a los dispositivos cliente.

Esta opción está recomendada para presentar el "desktop" como servicio, también bajo una conectividad permanente. Como ventajas, seguimos sin tener datos en el cliente, y con VDI conseguimos una experiencia de "PC" para el usuario.

En el apartado de las limitaciones, hay que considerar un elevado coste de adquisición (servidores, software, almacenamiento y un datacenter), seguimos con limitaciones en el área multimedia y es una tecnología con una inmadurez relativa.

En este apartado, la tecnologías Microsoft relacionadas es Microsoft Hyper-V de Windows Server 2008 y Windows Virtual Enterprise Centralized Desktop (VECD).
Windows Server 2008 R2 y Windows 7 ofrecen a las empresas la tecnología necesaria para poder ofrecer a los usuarios escritorios remotos basados en PCs virtuales (VDI). El usuario puede desde un PC de casa acceder a su "PC

corporativo" tal y como lo ve cuando está en la empresa sin ninguna pérdida de productividad.

Virtualización de Aplicaciones

En esta tercera opción ya vamos entrando en la tendencia de ofrecer aplicaciones como servicios, apropiadas para la movilidad y disponibilidad off-line. Como ventajas, destacan un mayor rendimiento de las aplicaciones, se resuelven los problemas de incompatibilidad de las mismas, ofrece un coste reducido (datacenter más software) y se simplifica la gestión de las licencias. En lo que a las limitaciones se refiere, aquí ya tenemos datos en el puesto de trabajo cliente (al menos durante el tiempo de ejecución) y ya es necesario gestionar el sistema operativo local.

Las tecnologías Microsoft aplicadas en este escenario son las de Microsoft Hyper-V Server, Microsoft Application Virtualization y Microsoft Enterprise Desktop Virtualization (MED-V).

Recomendamos la visualización de nuestro webcast a petición referenciado en el área de recursos, en el que se puede ver cómo MED-V proporciona una plataforma gestionable que garantiza la compatibilidad de aplicaciones mediante la virtualización de versiones anteriores del sistema operativo. Se puede ver cómo se pueden actualizar los escritorios manteniendo sus aplicaciones actuales.

OS Streaming

Aplicar el streaming del Sistema Operativo puede ser apropiado en escenarios de conectividad permantente, haciendo una provisión de "imagen" del PC. Como ventajas, ya tenemos una experiencia completa de PC para el usuario, el rendimiento de las aplicaciones es total (sólo dependemos de las características del PC local) y supone un coste reducido (en el datacentre). En las limitaciones, volvemos a tener datos en el cliente, al menos durante la ejecución, y nuestra red sufrirá una serie de importantes picos de tráfico en el arranque, a medida que los empleados se vayan incorporando al trabajo. Para este escenario, es necesaria tecnología de terceros, como Citrix Provisioning Server

Virtual Containers

Esta opción es apropiada para provisionar imágenes del PC, en escenarios de movilidad y disponibilidad off-line. Como ventajas destacan el óptimo

rendimiento de las aplicaciones, la posibilidad de disponer de imágenes múltiples por cliente y ofrecer costes reducidos

Como limitaciones, estamos hablando de tecnologías aún emergentes y que presentan cierta complejidad para aplicarlo a soluciones actuales. Antes de decantarse por alguna (o algunas) de las opciones presentadas, hay que tener en cuenta que no existe una solución para todo: ciertos usos y aplicaciones no operan ni rinden adecuadamente bajo determinadas arquitecturas.
Además, hay que tener en cuenta que las Tecnologías de la Información deben posibilitar la innovación del negocio mediante su aplicación razonable y racional, asegurando la evolución a futuras aplicaciones y medios de relación (pensemos en reconocimiento de voz, y eso enlaza con el último apartado de este documento, sobre las ventajas que aportan las Comunicaciones Unificadas en los entornos empresariales.

Registro

El registro diario de Acceso Remoto seguro

Modificaciones o cambios

Fecha anterior	**Cambios o modificaciones**	**Fecha del cambio**
n/a	Creación del procedimiento	05/11/2015
Elaborado por: **Nombre: M.Mora** **Cargo:** **Fecha:**	**Revisado por:** **Nombre: T. Tapia** **Cargo: Dir.Sistemas** **Fecha:**	**Aprobado por:** **Nombre : R. Tolozano** **Cargo: Rector** **Fecha:**
Firma	**Firma**	**Firma**

Objetivo

El objetivo principal del Modelo de Gestión de Incidentes de seguridad de la información es tener un enfoque estructurado y bien planificado que permita manejar adecuadamente los incidentes de seguridad de la información con el fin de poder asegurar la seguridad de la información.

Alcance

Es esencial de proveer y mantener la infraestructura de Tecnología de todas Las Empresas ha desarrollado las siguientes Políticas de Seguridad Informática que, a su vez, son un conjunto de normas enmarcadas en el ámbito jurídico y administrativo de Las Empresas. Estas normas inciden en la adquisición y el uso de los bienes y servicios informáticos, las cuales se deberán acatar por aquellas instancias que intervengan directa o indirectamente en ello.

Documentos de referencia

Metodología de gestión de seguridad

Responsables

Departamento de Sistemas es responsable de la oportuna solución a las diferentes eventualidades que se presenten por falla del acceso remoto seguro más explícitamente es el Administrador de redes, Jefe de Mantenimiento.

Definiciones

Ninguna

Desarrollo de Procedimiento

- Notificaciones de violaciones de seguridad

Es de carácter obligatorio para todo el personal (Fijo, Contratado), la notificación inmediata de algún problema o violación de la seguridad, del cual fuere testigo; esta notificación debe realizarse por escrito vía correo electrónico a La Gerencia y/o a los ATI y/o a la Gerencia de Contraloría, quienes están en la obligación de realizar las gestiones pertinentes al caso y de ser cierta la sospecha tomar las medidas adecuadas para solucionar el incidente.

Es responsabilidad de todo empleado que maneje datos o información a través de accesos debidamente autorizados, el cumplimiento de las políticas de control de acceso, puesto que estas descansan en el establecimiento de responsabilidades donde se incurra en alguna violación en materia de seguridad acarreando sanciones a quien las haya causado, puesto que esto ocasionaría perjuicios económicos a Las Empresas de diversa consideración. Es por ello que las personas relacionadas de cualquier forma con los procesos tecnológicos deben ser conscientes y asumir que la seguridad es asunto de todos y, por tanto, se debe conocer y respetar las Políticas de Seguridad.

Está fundamentado como una exigencia que el personal de la organización conozca sus responsabilidades, sanciones y medidas a tomar al momento de incurrir en alguna violación o falta, escrita en las Políticas de Seguridad firmado por el empleado o proveedor o cualquier empresa del grupo. Por esta razón se entenderá que sólo una adecuada política de seguridad tecnológica apoyará la concientización para obtener la colaboración de los empleados, haciéndoles conscientes de los riesgos que podemos correr y de la importancia del cumplimiento de las normas.

Bases de datos

Para la operación del software de red en caso de manejar los datos empresariales mediante sistemas de información, se deberá tener en consideración lo siguiente:

• Toda la información de Las Empresas deberá invariablemente ser operada a través de un mismo tipo de sistema manejador de base de datos para beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de presentarse alguna falla.

- El acceso a los sistemas de información, deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información de Las Empresas. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software.

- Se deben delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes.

- Los datos de los sistemas de información, deben ser respaldados de acuerdo a la frecuencia de actualización de sus datos, guardando respaldos históricos periódicamente. Es indispensable llevar una bitácora oficial de los respaldos realizados, asimismo, los CDs, DVDs, Blue Ray de respaldo deberán guardarse en un lugar de acceso restringido con condiciones ambientales suficientes para garantizar su conservación. En cuanto a la información de los equipos de cómputo personales, se recomienda a los usuarios que realicen sus propios respaldos en los servidores de respaldo externo (Google Drive) o en medios de almacenamiento alternos.

- Todos los sistemas de información que se tengan en operación, deben contar con sus respectivos manuales actualizados. Un técnico que describa la estructura interna del sistema así como los programas, catálogos y archivos que lo conforman y otro que describa a los usuarios del sistema y los procedimientos para su utilización.

Instalaciones de equipos de cómputo

La instalación del equipo de cómputo, quedará sujeta a los siguientes lineamientos:

- Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y tráfico de personas.

- El Área de Tecnología, así como las áreas operativas deberán contar con un plano actualizado de las instalaciones eléctricas y de comunicaciones del equipo de cómputo en red.

- Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.

- Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.

- En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.

Registro

Registró diario de Gestión y monitoreo de Seguridad

Modificaciones o cambios

Fecha anterior	**Cambios o modificaciones**	**Fecha del cambio**
n/a	Creación del procedimiento	05/11/2015
Elaborado por: **Nombre: M.Mora** **Cargo:** **Fecha:**	**Revisado por:** **Nombre: T. Tapia** **Cargo: Dir.Sistemas** **Fecha:**	**Aprobado por:** **Nombre : R. Tolozano** **Cargo: Rector** **Fecha:**
Firma	**Firma**	**Firma**

Objetivo

Ya comentamos que en el ciclo de vida del software se debían completar una serie de tareas para obtener un producto de software. A menudo, se dice que los distintos componentes de software deben pasar por distintas fases durante su ciclo de vida.

.Alcance

El desarrollo de programas que en muchos proyectos de desarrollo (no todos, por supuesto), la aplicación de una metodología brilla por su ausencia, siendo éste un concepto casi desconocido.

Documentos de referencia

- Procedimientos de desarrollo

Responsables

Departamento de desarrollo es responsable de la oportuna solución a las diferentes eventualidades que se presenten por falla desarrollo de programas.

Definiciones

Ninguna

Desarrollo de Procedimiento

. Hay una serie de metodologías que solemos llamar tradicionales, propuestas casi todas ellas con anterioridad a los años 90 del siglo XX, y que pretendían ayudar a los profesionales indicando pautas para realizar y documentar cada una de las tareas del desarrollo del software. Sin embargo, tienen casi todas

ellas un gran lastre: asumen que un proyecto informático es casi una extensión de un proyecto burocrático tradicional. Así pues, los pasos que sugieren para llevar a cabo cada tarea, aunque bienintencionados, están cargados de burocracia, reiteraciones, ambigüedades... No suelen tener en cuenta cosas como la calidad, la satisfacción, la competitividad, los beneficios. Fueron metodologías creadas en los años 70-80 pensando en los negocios de los años 50.

El mundo va ahora mucho más rápido: sólo los negocios inteligentes sobreviven... sólo los proyectos de software inteligentemente construidos lo hacen también. Ahora las comunicaciones son instantáneas... mundiales. La información fluye en tiempo real. Las empresas compiten al segundo.

El software ya tiene una cierta historia. Hemos aprendido mucho. Utilizamos conceptos abstractos para construir sistemas que van mucho más allá de los datos y los algoritmos.

La mayor parte de las metodologías tradicionales ya no funcionan. Están obsoletas desde casi todos los puntos de vista. Sólo algunas metodologías tradicionales han sido revisadas y adaptadas... y su funcionalidad suele estar limitada a proyectos poco innovadores.
Las metodologías surgidas desde los 90 hasta aquí suelen tener otra mentalidad... una cierta agilidad. Siendo conscientes de lo cambiante y amplio que es el mundo del software, una metodología debe ser lo suficientemente precisa como para que todo el mundo la pueda seguir y sea de utilidad como pauta común, pero también debe ser lo suficientemente adaptable como para poder aplicarse en distintos proyectos, y lo suficientemente sencilla como para que no resulte muy gravosa su utilización, pero lo suficientemente completa y compleja como para que la utilización por parte del equipo sea provechosa... En una palabra: *agilidad*.

Aunque el término de agilidad es muy discutible, es indudable que las metodologías "modernas" responden a otra mentalidad completamente distinta.

Así a la pregunta de "¿Qué metodología utilizar?"... pues podemos dar una orientación dependiendo de tu situación:

- Si formas parte de un equipo de desarrollo en un proyecto grande y te toca decidir qué metodología hay que utilizar significa que tienes un puesto de responsabilidad. Escoge una metodología moderna, bien definida, que dé respuesta a las necesidades del proyecto.
- Si ocupas un puesto de decisión en un proyecto grande pero institucional, quizá de una administración pública, o un proyecto estructural de una gran empresa, es decir, uno de esos proyectos 'pesados' cuyo punto clave es el tratamiento masivo de datos, quizá la metodología esté previamente escogida. En ese caso, hay que limitarse a seguirla. Esto suele ocurrir en proyectos de este tipo porque involucran a muchos actores con un perfil no técnico, y una enorme cantidad de burocracia. Son proyectos poco competitivos, y la inercia corporativa tiende a fijar una metodología para ellos -siempre la misma dentro de la misma institución- con el fin de uniformizar el desarrollo.
- Si formas parte de un equipo de desarrollo en un proyecto grande y no ocupas un puesto de responsabilidad, no deberías decidir qué metodología utilizar: alguien lo decidirá por ti. Si nadie toma esa decisión y en el proyecto no se escoge una metodología, o al menos, se fijan algunas pautas metodológicas generales, entonces... ¡Mucho ánimo!... el proyecto en el que estás involucrado está destinado al fracaso. Intenta vivirlo de la mejor manera posible y trata de aprender de la experiencia.
- Si formas parte de un equipo pequeño en un proyecto pequeño, lo mejor es consensuar la metodología a utilizar. Incluso, combinar buenas ideas de más de una.

Plan de contingencia para: Reinicio de servidores

Antecedentes

La infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función del negocio.

Los procedimientos relevantes a la infraestructura informática, son aquellas tareas que el personal realiza frecuentemente al interactuar con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.).El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre

Objetivo

- Establecer mecanismos y procedimientos para proporcionar confidencialidad, integridad y disponibilidad de la información.
- Estimular la creación de una cultura de seguridad en Informática, así como fomentar la ética entre el personal de la empresa.
- Definir los requerimientos mínimos de seguridad en cada área, dependiendo del tipo de información que se procese: confidencial, restringida, de uso interno, general o público, estableciendo los procedimientos para identificación y uso de cada categoría de información.
- Promover el establecimiento de procedimientos alternos en previsión a contingencias de cualquier naturaleza que garanticen en la medida de lo posible, la continuidad del procesamiento de la información y la prestación de servicios, mismos que al incorporarse al presente documento lo irán enriqueciendo y de esta manera se logrará contar cada vez con una mejor herramienta que apoye a superar las contingencias que se presenten.

Paso

- Bienes susceptibles de daño.
- Se puede identificar los siguientes bienes afectos a riesgos:
- a) Personal.
- b) Hardware.
- c) Software y utilitarios.
- d) Datos e información.
- e) Documentación.
- f) Suministro de energía eléctrica.
- g) Suministro de telecomunicaciones.
- Daños.
- Los posibles daños pueden referirse a:
- 1) Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes, sea por causas naturales o humanas.
- 2) Imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales, por ejemplo, cambios de claves o códigos de acceso, datos maestros claves, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.
- 3) Divulgación de información a instancias fuera de la empresa y que afecte su patrimonio estratégico comercial y/o Institucional, sea mediante robo o infidencia.

Registro

Registro varía dependiendo de las necesidades del desarrollo de programas

Modificaciones o cambios

Fecha anterior	**Cambios o modificaciones**	**Fecha del cambio**
n/a	Creación del procedimiento	05/11/2015
Elaborado por: **Nombre: M.Mora** **Cargo:** **Fecha:**	**Revisado por:** **Nombre: T. Tapia** **Cargo: Dir.Sistemas** **Fecha:**	**Aprobado por:** **Nombre : R. Tolozano** **Cargo: Rector** **Fecha:**
Firma	**Firma**	**Firma**

Instituto Tecnológico Bolivariano Registro de CONESUP 09-030	**PROCEDIMIENTO**		**Pagina 1/4**
	CONTINGENCIA REINICIO DE SERVIDORES		
Código: SIS-005-2015	**Revisión Ant.: N/A**	**Vigencia: Nov 2015**	

Objetivo

Establecer un adecuado sistema de seguridad física y lógica en previsión de desastres

.**Alcance**

Los procedimientos relevantes a la infraestructura informática, son aquellas tareas que el personal realiza frecuentemente al interactuar con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.).El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre

Documentos de referencia

- Contingencias para reinicio de servidores

Responsables

El administrador de red es responsable de la oportuna solución a las diferentes eventualidades que se presenten por falla de los servidores.

Definiciones

Ninguna

Desarrollo de Procedimiento

Establecer mecanismos y procedimientos para proporcionar confidencialidad, integridad y disponibilidad de la información.

Estimular la creación de una cultura de seguridad en Informática, así como fomentar la ética entre el personal de la empresa.

Definir los requerimientos mínimos de seguridad en cada área, dependiendo del tipo de información que se procese: confidencial, restringida, de uso interno, general o público, estableciendo los procedimientos para identificación y uso de cada categoría de información.

Promover el establecimiento de procedimientos alternos en previsión a contingencias de cualquier naturaleza que garanticen en la medida de lo posible, la continuidad del procesamiento de la información y la prestación de servicios, mismos que al incorporarse al presente documento lo irán enriqueciendo y de esta manera se logrará contar cada vez con una mejor herramienta que apoye a superar las contingencias que se presenten.

Paso

Bienes susceptibles de daño.

Se puede identificar los siguientes bienes afectos a riesgos:

a) Personal.

b) Hardware.

c) Software y utilitarios.

d) Datos e información.

e) Documentación.

f) Suministro de energía eléctrica.

g) Suministro de telecomunicaciones.

Daños.

Los posibles daños pueden referirse a:

1) Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes, sea por causas naturales o humanas.

2) Imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales, por ejemplo, cambios de claves o códigos de acceso, datos maestros claves, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.

3) Divulgación de información a instancias fuera de la empresa y que afecte su patrimonio estratégico comercial y/o Institucional, sea mediante robo o infidencia.

Registro

Registro varía dependiendo de las necesidades de las necesidades del mantenimiento de las aulas y bienes informáticos

Modificaciones o cambios

Fecha anterior	**Cambios o modificaciones**	**Fecha del cambio**
n/a	Creación del procedimiento	05/11/2015
Elaborado por: **Nombre: M.Mora** **Cargo:** **Fecha:**	**Revisado por:** **Nombre: T. Tapia** **Cargo: Dir.Sistemas** **Fecha:**	**Aprobado por:** **Nombre : R. Tolozano** **Cargo: Rector** **Fecha:**
Firma	**Firma**	**Firma**

Instituto Tecnológico Bolivariano Registro de CONESUP 09-030	**PROCEDIMIENTO**		**Pagina 1/5**
	CONTINGENCIA MANTENIMIENTO EN AULA		
Código: SIS-006-2015	**Revisión Ant.:jul 2012**	**Vigencia: Nov 2015**	

Objetivo

Después de revisar el sistema, debería evaluarse minuciosamente para garantizar que todos sus componentes se desempeñen de acuerdo a los requerimientos específicos y que trabaje adecuadamente aunque se usen otras funciones o se introduzca información errónea.

.**Alcance**

Los contratos informáticos pueden referirse tanto a Los contratos informáticos bienes (hardware o software) como a servicios informáticos (tales como mantenimiento preventivo, correctivo o evolutivo; desarrollo y evitar fallas

Documentos de referencia

- Planes de contingencia ITB

Responsables

Departamento de soporte técnico es responsable de la oportuna solución a las diferentes eventualidades que se presenten por falla desarrollo de programas.

Definiciones

Ninguna

Desarrollo de Procedimiento

Servicios de mantenimiento de equipo de cómputo

Es la limpieza externa del equipo como es gabinete y dentro del gabinete (tarjeta madre, cables, fuente de poder, unidades de cd, discos duros, memorias ram, ventiladores, etc) y hablando tecnicamente es mantener optimo el funcionamiento del sistema operativo impidiendo que se haga lento el sistema, esto se puede definir como examinar los discos duros para encontrar y eliminar virus, eliminar programas y archivos inservibles como son archivos temporales de i Internet, cookies, etc.

Servicios de soporte técnico

El soporte técnico es un rango de servicios que proporcionan asistencia con el hardware o software de una computadora, o algún otro dispositivo electrónico o mecánico. En general los servicios de soporte técnico tratan de ayudar al usuario a resolver determinados problemas con algún producto en vez de entrenar o personalizar. En general, el servicio de soporte técnico sirve para ayudar a resolver los problemas que puedan presentárseles a los usuarios, mientras hacen uso de servicios, programas o dispositivos.

La mayoría de las compañías que venden hardware o software, ofrecen servicio técnico por teléfono u otras formas online como e-mails o sitios web.

Las compañías e instituciones también tienen generalmente soporte técnico interno para empleados, estudiantes y otros asociados.

Cableado de redes de voz y datos

El concepto de cableado estructurado, red de voz y datos, hace referencia al soporte físico de un sistema de comunicaciones que posee unas características determinadas como son:

Disponer de tomas estandarizadas para voz, datos u otros servicios telemáticos.

Las tomas son distribuidas por múltiples puntos de la empresa previendo futuras conexiones y ampliaciones de la red de voz y datos.

Este sistema puede distribuirse en una planta, en un edificio o en un campus de edificios.

La administración se centraliza en puntos donde confluyen distintos tramos de cable (UTP, FTP, ETC.) y/o Fibra óptica(FO).

Los cables, la FO, los conectores así como los tramos completos (enlaces y canales) están normalizados.

Una red de voz y datos, sistema de cableado estructurado, unifica en una misma infraestructura de telecomunicaciones los servicios de voz, datos y video con un sistema de gestión centralizado, aportando importantes beneficios para las empresas:

Simplificación de la infraestructura de comunicaciones.

Ahorro en los costes de mantenimiento.

Optimización de la gestión.

Flexibilidad y modularidad, lo que permite facilidad de ampliación.

PROGRAMAS OFIMÁTICOS

Se llama ofimática el conjunto de técnicas, aplicaciones y herramientas informáticas que se utilizan en funciones de oficina para optimizar, automatizar y mejorar los procedimientos o tareas relacionados.

Las herramientas ofimáticas permiten idear, crear, manipular, transmitir y almacenar información necesaria en una oficina. Actualmente es fundamental que estas estén conectadas a una red local y/o a internet.

Cualquier actividad que pueda hacerse manualmente en una oficina puede ser automatizada o ayudada por herramientas ofimáticas: dictado, mecanografía, archivado, fax, microfilmado, gestión de archivos y documentos, etc.

Herramientas y procedimientos ofimáticos

Procesamiento de textos: Ver Procesador de texto.

Hoja de cálculo

Herramientas de presentación multimedia.

Base de datos.

Utilidades: ag

Sistema de Bases de Datos

Un Sistema de Bases de Datos (SBD) es una serie de recursos para manejar grandes volúmenes de información, sin embargo no todos los sistemas que manejan información son bases de datos.

Un sistema de bases de datos debe responder a las siguientes características:

Independencia de los Datos. Es decir, que los datos no dependen del programa y por tanto cualquier aplicación puede hacer uso de los datos.

Reducción de la Redundancia. Llamamos redundancia a la existencia de duplicación de los datos, al reducir ésta al máximo conseguimos un mayor aprovechamiento del espacio y además evitamos que existan inconsistencias entre los datos. Las inconsistencias se dan cuando nos encontramos con datos contradictorios.

Registro

Registro varía dependiendo de las necesidades de las necesidades del mantenimiento de las aulas y bienes informáticos

Modificaciones o cambios

Fecha anterior	**Cambios o modificaciones**	**Fecha del cambio**
n/a	Creación del procedimiento	05/11/2015
Elaborado por: **Nombre: M.Mora** **Cargo:** **Fecha:**	**Revisado por:** **Nombre: T. Tapia** **Cargo: Dir.Sistemas** **Fecha:**	**Aprobado por:** **Nombre : R. Tolozano** **Cargo: Rector** **Fecha:**
Firma	**Firma**	**Firma**

Instituto Tecnológico Bolivariano Registro de CONESUP 09-030	**PROCEDIMIENTO**		**Pagina 1/4**
	CONTINGENCIA INSTALACIÓN DE PROGRAMAS		
Código: SIS-007-2015	**Revisión Ant.:jul 2012**	**Vigencia: Nov 2015**	

Objetivo

Ayudar a resolver problemas y a generar nuevas ideas, nos proporciona el poder de crear y colaborar. En definitiva, el software ha hecho posible que pos procesos productivos.

.**Alcance**

En la presente sociedad del conocimiento, todos los procesos productivos sin excepción, se hayan vinculados a la informática, y por tanto a los programas de ordenador que hacen posible su desarrollo.

Documentos de referencia

Responsables

Departamento de soporte técnico es responsable de la oportuna solución a las diferentes eventualidades que se presenten por falla o falta de instalación de programas.

Definiciones

Ninguna

Desarrollo de Procedimiento

Licencia de uso

Una licencia de software representa el permiso del fabricante para la instalación y utilización de su producto en un ordenador o sistema informático. La licencia contiene los términos y condiciones que regulan la utilización del software, incluido el ámbito de los derechos de la licencia y cualquier limitación relacionada con esta, como su propósito, el lugar de uso y el hardware que se empleará. Las licencias normalmente contienen una definición del producto, términos de aceptación y alguna cláusula de garantía. Los acuerdos más complejos también pueden incluir calendarios de implantación, cláusulas de confidencialidad y condiciones de pago. Por lo general, una licencia de software otorgará un derecho no exclusivo al licenciatario (la empresa usuaria) para que un número concreto de usuarios utilicen una copia del software. Salvo que se indique lo contrario, estará estrictamente prohibida la copia y distribución de dicho software a otros usuarios u ordenadores.

Son muchos los conceptos erróneos en torno al concepto de "titularidad" y propiedad intelectual. El licenciatario nunca adquiere derecho de propiedad alguno sobre el programa. Sin embargo, sí obtendrá el derecho a utilizar el software de acuerdo con los términos y condiciones que especifique el titular de la propiedad intelectual, y lo que estipule la ley vigente. La única excepción a lo anterior se producirá cuando se haya desarrollado un software a medida en nombre de una empresa o particular. Por lo general, las empresas suelen desprenderse de aquella documentación relativa a la prueba de su compra. Es de vital importancia poder probar que la empresa cuenta con licencias válidas de todos sus activos de software. El no hacerlo podría conducir hacia los riesgos que más adelante se describen. Para que conste la prueba de compra y su derecho legal a utilizar el software, deberá asegurarse de que su empresa siempre tiene: - Soporte original (CD’s de instalación) - Contratos de licencia, a menudo denominado "Acuerdo de licencia de usuario final" o EULA (del

inglés End User License Agreement) - Certificado de autenticidad - Manuales y guías de usuario - Copias impresas de cualquier acuerdo de licencia formalizado “on line” - Facturas y recibos de compra originales de las licencias adquiridas.

Escenarios de incumplimiento

Se producen escenarios de incumplimiento, cuando existen actividades de copia, uso, distribución o comercialización de un programa de ordenador de cualquier forma no permitida por la Ley de la Propiedad Intelectual o por el fabricante del programa, según lo establecido en el contrato de licencia de uso.

Las siguientes actividades implican que la empresa se encuentre en un escenario típico de incumplimiento:

- Copiar o distribuir un programa de ordenador o la documentación que le acompaña, incluidas aplicaciones, datos, códigos y manuales, sin permiso expreso o licencia del propietario de los derechos de explotación.

- Utilizar un programa sin la correspondiente licencia o autorización del fabricante, con independencia de que se utilice en un solo ordenador o en varios de forma simultánea.

- Utilizar programas de ordenador en un número de copias, o por un número de usuarios, superior al autorizado por el fabricante en sus contratos o licencias de uso.

Registro

Registro varía dependiendo de las necesidades de las necesidades del mantenimiento de las aulas y bienes informáticos

Modificaciones o cambios

Fecha anterior	**Cambios o modificaciones**	**Fecha del cambio**
n/a	Creación del procedimiento	05/11/2015
Elaborado por: **Nombre: M.Mora** **Cargo:** **Fecha:**	**Revisado por:** **Nombre: T. Tapia** **Cargo: Dir.Sistemas** **Fecha:**	**Aprobado por:** **Nombre : R. Tolozano** **Cargo: Rector** **Fecha:**
Firma	**Firma**	**Firma**