AUDITORIA INFORMÁTICA INTERNA EN NUESTRO DEPARTAMENTO

Carmen Janeth Padilla Vedia [1]

Docente investigadora del Departamento de Informática y Sistemas - UAJMS
Dirección para correspondencia: padillac555@gmail.com

(Investigación aplicada a La Avenida Sagredo - Barrio German Busch - Tarija)

Resumen

La seguridad es primordial en el ser humano y en la realización de cualquier proyecto o situación de la vida, de forma que no queda exento el área de informática dentro de las organizaciones públicas o privadas con o sin fines de lucro contribuyendo a prevenir, mantener el funcionamiento y resguardar los activos de las mismas.
La seguridad informática es una necesidad presente en cualquier institución, cuando se tienen protocolos, controles y procedimientos que permitan verificar que los objetivos de continuidad de servicio, confidencialidad y seguridad de la información, se cumpliría satisfactoriamente con las características primordiales de la información, y así se prevería la alteración de sistemas, ataques y accesos no autorizados.

Las empresas o instituciones en nuestro medio actualmente manejan su información y la administran por medio se software, por tanto es necesario que todas implanten una evaluación de riesgos para la información con el propósito de proteger la integridad y cumplir con los controles de políticas de seguridad. La seguridad informática se presenta como una necesidad que se fundamenta en el establecimiento de controles e implantación de procedimientos y métodos con el objetivo de administrar y proteger los activos de la información.

Las empresas están expuestas a riesgos potenciales que hay que concientizar, dar a conocer y atacar posteriormente con políticas del tipo preventivas, detectivas y hasta correctivas para así lograr una administración de la información más eficaz y segura.

Palabras clave:

SAI = Sistema de alimentación ininterrumpida
ISO = Organización Internacional de Estandarización
COBIT = Objetivos de Control para la Información y Tecnologías Relacionadas
ITIL = Information Technology Infrastructure Library
COSO = The Committee of Sponsoring Organizations of the Treadway Commission's Internal Control - Integrated Framework

Problema de Investigación

Nuestras empresas tienen riesgo de perder información, esto podría detener su operación, deteniendo procesos de producción o administrativos, para ello es necesario proteger la información, haciendo que las unidades de auditoria no solo se concentren en auditorias financieras, sino que también se planifiquen y ejecuten los controles internos informáticos, bien sabemos que existen diferentes maneras o métodos de proteger un sistema de información, todas estas partes del sistema de seguridad deben trabajar en conjunto para asegurar la informática de la empresa. Para mejorar la función del área de auditoria o como se la nombre en las organizaciones de nuestro medio, esta área debería incluir la auditoria interna informática y no así solo auditoría financiera como ocurre en la mayoría de nuestras instituciones ocasionando esta situación problemas que repercuten en la administración e imagen propia de la empresa u organización, ya que hoy por hoy nuestras organizaciones en su mayoría administran la información haciendo uso de medios electrónicos.

Fundamentación Teórica y Metodológica

Introducción

En todo objeto de estudio de la humanidad, se necesita estabilidad y protección de información o bienes, en informática sabemos que la herramienta principal que ayudo a su popularidad en el mundo, son las computadoras, cualquiera que sea la categoría

Esto hace que las organizaciones anglosajonas y europeas se preocupen por proteger los activos involucrados en la administración y uso de la información , sin embargo esto no sucede de la misma manera en nuestro departamento con nuestras instituciones por distintas razones que trataremos que explicarlas a continuación.

La administración de información en Tarija

Las empresas o instituciones en nuestro medio actualmente manejan su información y la administran por medio se software, por tanto es necesario que todas implanten controles internos que disminuyan los riesgos potenciales en la administración de la información con el propósito de proteger la integridad y cumplir con los controles de políticas de seguridad. La seguridad informática se presenta como una necesidad que se fundamenta en el establecimiento de controles e implantación de procedimientos y métodos con el objetivo de administrar y proteger los activos de la información.

“La seguridad informática solo brinda áreas de oportunidad, en los sistemas informáticos y no brinda por si sola seguridad en la información de la organización, la seguridad informática, no puede por sí misma. De ahí que el hacer conciencia para que las áreas comprometidas con esta labor asuman las funciones y responsabilidades que conlleva la actividad de auditoria informática interna dentro de las diferentes organizaciones que hacen vida orgánica en nuestro departamento es crucial.

Nuestras empresas están expuestas al riesgo de perder información, esto podría detener su operación, deteniendo procesos de producción o administrativos, para ello es necesario proteger el funcionamiento de la información, existen diferentes maneras o métodos de proteger un sistema de información, todas estas partes del sistema de seguridad deben trabajar en conjunto para asegurar la informática de la empresa, de ahí que un elemento indispensable y poco frecuente en nuestras instituciones es el área de auditoria interna informática que al operar como tal , reduzca el riesgo informatico.

La seguridad informática existe solo si se juntan todos los elementos y métodos que la hacen posible ya que cualquier método utilizado por sí solo no puede abarcar todos los puntos vulnerables de los sistemas de información, así lo da a entender, Hallberg (2003, p.97). “La seguridad informática solo brinda áreas de oportunidad, en los sistemas informáticos y no brinda por si sola seguridad en la información de la organización, la seguridad informática, no puede por sí misma proporcionar la protección para su información”.

Este trabajo de investigación trata de hacer notar la falta del área de auditoria interna informática en nuestras instituciones y el impacto que esto causa o puede causar.

La manera en que manejamos la seguridad de la información ha evolucionado con el tiempo, a medida que nuestra sociedad y tecnología evolucionan, por ello es importante comprender y aplicar esta evolución para lograr procedimientos más seguros y efectivos que van en bien de las instituciones , ya que lo que en algún momento es seguro con el paso del tiempo ya no lo es, como lo describe Maiwald (2003, p.8) “La seguridad era suficiente cuando la información no estaba en la nube , pero al cambio de tecnologías estos ya no lo es, la mayor parte de los activos de la información de las organizaciones migraron hacia ellas en formato electrónico, cambiando por completo la idea de seguridad en la información”, es por esto que pretendemos mostrar y describir los elementos y características que conforman la seguridad informática en nuestras instituciones.

La mayoría de las empresas o instituciones en nuestro departamento hoy en día administran su información, con ayuda de la tecnología construyendo sistemas de información, para que los colaboradores de las empresas puedan acceder rápidamente a toda la información empresarial, confiando completamente la información a los sistemas computacionales.

Cuando no se conoce el alcance que tienen los sistemas informáticos, ni lo vulnerables que pueden ser, si son expuestos a Internet por los mismos empleados de la organización, puede haber fuga de información hacia el exterior, al hablar de seguridad informática podemos hablar desde un software que restringe otros programas malignos, llamado antivirus, un software que previene que personas foráneas logren acceder, llamado firewall, hasta seguridad física, que bien podría ser un buen edificio con controles de acceso y seguridad privada que restrinjan el acceso a personas.

Auditoria informática interna

La auditoría interna es el examen crítico, sistemático y detallado de los sistemas de información de una organización; realizadas por profesionales con vínculos laborales con la misma. Estos profesionales utilizan técnicas determinadas con el objetivo de emitir informes y formular sugerencias para el mejoramiento de la entidad o negocio. Las auditorías internas son servicios que reportan al más alto nivel de la gerencia de la organización y tienen características de función asesora de control; por tanto no pueden ni deben tener autoridad sobre ningún funcionario de la empresa, a excepción de los que forman parte del personal de la oficina de auditoría interna. Tampoco, deben involucrarse o comprometerse con las operaciones de los sistemas de la empresa, pues su función es evaluar y opinar sobre los mismos; para que la alta gerencia tome las medidas necesarias para su mejor funcionamiento.

Estándares y Normas para Asegurar 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 confidencialidad, disponibilidad e integridad.

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 pueden ser consideradas como base para construir un modelo de seguridad.

ISO 17.799

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.

ITIL

Acrónimo de “Information Technology Infrastructure Library”, ITIL es una norma de mejores prácticas para la administración de servicios de Tecnología de Información (TI), desarrollada a finales del año 1980 por entidades públicas y privadas con el fin de considerar las mejores prácticas a nivel mundial.

COSO

La normativa COSO, acrónimo de The Committee of Sponsoring Organizations of the Treadway Commission's Internal Control - Integrated Framework, está principalmente orientada al control de la administración financiera y contable de las organizaciones. Sin embargo, dada la gran cercanía que hoy existe entre esta área y los sistemas de información computarizados, es que resulta importante entender el alcance y uso de esta norma. el Informe COSO es un documento que contiene directivas e indicaciones para la implantación, gestión y control de un sistema de Control Interno, con alcances al área informática.

ISO Serie 27000

A semejanza de otras normas ISO, la 27000 es una serie de estándares, que incluye (o incluirá, pues algunas partes aún están en desarrollo), definiciones de vocabulario (ISO 27000), requisitos para sistemas de gestión de seguridad de la información (ISO 27001), guía de buenas prácticas en objetivos de control y controles recomendables de seguridad de la información (ISO 27002), una guía de implementación de SGSI (Sistema de Gestión en Seguridad de la Información) junto a información de uso del esquema PDCA (Plan, Do, Check, Act) [6] (ISO 27003), especificación de métricas para determinar la eficacia de SGSI (ISO 27004), una guía de técnicas de gestión de riesgo (ISO 27005), especificación de requisitos para acreditación de entidades de auditoria y certificación de SGSI (ISO 27006), una guía de auditoria de SGSI (ISO 27007), una guía de gestión de seguridad de la información para telecomunicaciones (ISO 27011), una guía de continuidad de negocio en cuanto a TIC (ISO 27031), una guía de ciber-seguridad (ISO 27032), una guía de seguridad en redes (ISO 27033), una guía de seguridad en aplicaciones (ISO 27034), y una guía de seguridad de la información en el sector sanitario (ISO 27799).

Políticas de Seguridad

La seguridad informática se enfoca en la protección y la privatización de sus sistemas y en esta se pueden encontrar dos tipos: La seguridad lógica que se enfoca en la protección de los contenidos y su información y la seguridad física aplicada a los equipos como tal, ya que el ataque no es estrictamente al software y también al hardware y también la infraestructura informática es una parte fundamental para la preservación del activo más valioso que es la información, así mismo se busca mantener la confidencialidad, integridad, autenticidad, y disponibilidad que son los datos recordando símbolos que representan hechos, situaciones, condiciones o información es el resultado de procesar o transformar los datos la información es significativa para el usuario.

Atendiendo a esta definición es importante tener políticas de seguridad, bien concebidas y efectivas, que puedan proteger la inversión y los recursos de información de las instituciones locales. Vale la pena implementar políticas de seguridad si los recursos y la información merecen protegerse, por eso es importante que exista la unidad de auditoria interna quien tiene la función de implementar y controlar los controles internos de manera diaria.

Que podemos hacer para garantizar políticas de seguridad?

Asegurar que todos los involucrados conozcan sus funciones y responsabilidades y a medida que introducimos controles internos, irán apareciendo nuevos en función a las necesidades y amenazas latentes, esto normalmente sucede debido a que no todas las amenazas pueden ser anticipadas, entonces hay que estar alertas a la presencia de todo tipo de posible amenaza a la que este expuesta y sea posible de acaecer.

Las políticas deben estar diseñadas por niveles de seguridad por ejemplo desde proteger una contraseña hasta protecciones físicas y lógicas como por ejemplo cifrado de datos, pistas de auditoria.

Sistemas de Protección

Un sistema de protección es algo que toda empresa debe tener para evitar accidentes de todo tipo y así minimizar los posibles riesgos a la infraestructura o a la información que puedan ser causados por incendios o fallas eléctricas o cualquier otro riesgo, otro de los que pueden ser usados son los llamados sistemas contra incendios y además del uso de extintores y sistemas convencionales antiincendios convencionales, hay otros tipo de sistemas más eficaces, como la inserción de gases nobles o la extracción de oxígeno, que preservan mejor los equipos para que no sean alcanzados por el fuego evitando así el contacto con el líquido de los extintores o el agua. Si la empresa u organización es suficientemente grande, puede tener un sistema contra incendios centralizado, que normalmente está en una habitación y mediante una bomba surte agua a todas las plantas del edificio en caso de incendio.

En nuestras instituciones dadas sus características generales podemos mencionar algunas que consideramos pueden ser efectivas:

- **Sistemas de protección eléctrica.** Para el correcto funcionamiento de un sistema informático es primordial que la corriente eléctrica sea adecuada. Por un lado es imposible asegurar que no haya un fallo en la tensión eléctrica y por otro la corriente puede sufrir perturbaciones. Todo esto puede dar problemas en el equipo , como perdida de información hasta fallos en el hardware, dependiendo del problema que se haya producido en la red eléctrica, también podemos descartar, entre otros: El corte de suministro eléctrico, que es la pérdida total de la tensión, Picos de tensión altos, llamados también sobretensión, que se dan cuando el valor de la tensión es superior al 110% del valor nominal, Picos de tensión bajos, llamados también caídas de tensión, que se dan cuando el valor de la tensión es inferior al 80% del valor nominal, Interferencias en la tensión, que se le suele denominar también fluctuaciones de tensión o ruidos, Microcortes, que son cortes de corriente durante un tiempo muy pequeño.
- **Sistemas de alimentación ininterrumpida.** El principal funcionamiento de los sistemas de alimentación ininterrumpida es preservar los equipos ante cualquier percance eléctrico. Estos equipos dan corriente eléctrica al sistema informático en caso de corte, algunos de ellos, corrigen las alteraciones en la tensión eléctrica, además de poder apagar los equipos de forma correcta si fuera necesario. Dos cosas que hay que tomar en cuenta para elegir un SAI (Sistema de alimentación ininterrumpida) son: el tiempo de autonomía de funcionamiento una vez que se produzca el corte de suministro eléctrico, el otro es la potencia, que deberá ser la necesaria para poder atender el consumo de todos los equipos que queramos proteger.
- **Clúster de servidores.** Un clúster de servidores es un conjunto de ordenadores conectados por una red de forma que funcionan como si tratase de uno solo. Tienen un alto rendimiento y una alta escalabilidad. Los equipos que componen el conjunto no tienen por qué tener ni el mismo hardware ni el mismo software, es decir, pueden ser equipos diferentes unos de otros. Las funciones que puede hacer un clúster son, además de un alto rendimiento y eficiencia, garantizar que en el movimiento en que se produzca un fallo hardware en alguno de los servidores del conjunto, no peligre el buen funcionamiento ni la disponibilidad del sistema informático, porque la operación que se estaba realizando en uno de los servidores del clúster puede pasar a realizarla otro.
- **Sistemas de identificación.** Un sistema de identificación es un método para el acceso al sistema informático, como a las instalaciones donde este se encuentre físicamente. El uso de técnicas y procedimientos se usan para controlar el acceso a las personas que quieran acceder al sistema o al usuario que accede localmente o de forma remota. Algunas de las herramientas destinadas a tal fin son: la firma electrónica, el certificado digital y otros que no son incorporados en nuestro medio, sin embargo son efectivos.
- **Seguridad en el acceso al sistema informático.** Es muy importante evitar el acceso no autorizado tanto al sistema informático como al recinto o lugar donde se encuentre ubicado, es una parte muy importante dentro de la seguridad y para eso existen los sistemas de protección.

Todas estas medidas de protección formaran parte de la seguridad activa, ya que se utilizan para evitar el acceso de un usuario no autorizado que podría comprometer tanto la privacidad como la integridad de la información contenida en el sistema informático.

- **Sistemas de control de acceso.** Algunos sistemas de control de acceso pueden ser: guardias y cámaras de seguridad que son utilizados para evitar el acceso al edificio tanto exterior o interior y así controlar el acceso a lugares restringidos. El uso de llaves para acceder al edificio o a la habitación donde se encuentran los equipos, así como llaves para bloquear el equipo en si. También se usan claves de acceso o contraseñas para entrar a lugares protegidos o cuentas de usuario. Los sistemas de contraseñas para entrar en un equipo informático son utilizados para que los sistemas de contraseñas sean correctos y cumplan su función.

El nivel de seguridad que se adopte implica a menudo consecuencias ligadas a: restricciones para los usuarios, que deberán autenticarse antes de acceder a algunos recursos. La carga financiera que representa la adquisición de los programas de protección.

El tiempo de trabajo necesario para implementar estas soluciones y una mayor complejidad de la infraestructura. Por este motivo una buena política de seguridad podría ser una solución adaptada a sus necesidades, suficientemente potente para protegerle, sin paralizar la empresa debido a restricciones demasiado importantes.

La implementación de medidas de seguridad adecuadas para proteger a una empresa normal, representa un trabajo considerable pero no supone mayores problemas. Es una misión accesible para cualquier persona que disponga un buen nivel de competencia informática.

Por qué debe considerarse un área de auditoria interna informática

Información mostrada en páginas web de empresas tarijeñas nos muestran que a nivel departamental existen cerca de 46 empresas del departamento que cuentan con sus páginas Web y éstas van desde empresas del rubro de automotores, vinos, industria, educación, turismo, hoteles, instituciones públicas y otras.

Según el especialista nacional, Álvaro Luksic, la prensa tarijeña, es el rubro que más empeño ha puesto a su presencia online en los últimos años. Entre algunas de las páginas web más visitadas se encuentran las del diario El País e y la de la universidad Juan Misael Saracho.

Existiendo también sistemas que no se encuentran en la web, pero igualmente importantes en la administración y control de las instituciones locales. Esta necesidad tecnológica cada vez más imprescindible nos hace pensar el incorporar la unidad de auditoria interna informática que controle diariamente las actividades involucradas con TIC, permitiendo lograr más eficiencia y eficacia en nuestras instituciones. Adicionalmente, las empresas deben evitar una serie de riesgos de seguridad, entre los que incluyen robo de identidad, fuga de información, fraude y otros.

Importancia de implementar controles internos

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 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.

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 de cada organización.

Estos controles deben estar abalados por políticas, procedimientos e instructivos que permitan operar de manera clara, precisa y sin ambigüedades de tal forma de asegurar el correcto cumplimiento de los controles y de la evidencia que de ellos se desprenda.

Conclusiones

De acuerdo a lo expuesto en los párrafos anteriores podemos evidenciar la importancia que radica el contar con una área dedicada exclusivamente a controlar las actividades rutinarias y que hacen a la institución, dándole la opción de tener un control sobre estas actividades y poder mejorar el funcionamiento en general de toda la institución, ya que el área de auditoria informática interna tendrá constantemente cubierta la parte de controles internos, permitiendo dotar de un seguimiento sistemático y controlado de las actividades que la institución desempeña como parte del rubro al que pertenece.
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.

Bibliografía

García, Alfonso – Alegre, María del Pilar (2011).Seguridad Informática.Paraninfo.España.

Hallberg Bruce A, (2003). “Fundamentos de redes”, Editorial McGraw-Hill. Primera edición. México DF.

Kendall Kenneth E. (2005). “Análisis y diseño de sistemas”, Editorial Pearson. Sexta edición.

Ochoa Ovalles, S. y Cervantes Sánchez, O. Seguridad informática. Contribuciones a las Ciencias Sociales. http://www.eumed.net/rev/cccss/21/oocs.html

Rosales Uriona Guido. (2002). Estrategias para la seguridad de la información. Editorial Yanapti. Primer edición. La Paz Bolivia.

Royer, Jean-Mark, (2004). Seguridad en la informática de la empresa. ENI. Barcelona España.

Maiwald Eric, (2005). “Fundamentos de seguridad en redes”, Editorial McGraw-Hill, primera edición. México DF.

Telecomunicaciones en Bolivia. (1 de Febrero de 2015). Noticias de Tecnología y Telecomunicaciones. http://www.telecombol.com/2015/02/las-empresas-tarijenas-se-quedan-en-el.html

emagister.com Wikilearning Comunidades de Wikis Libres para Aprender. http://www.wikilearning.com/articulo/conociendo_al_sidunea-caracteristicas_tecnologicas/13402-3
www.eumed.net/rev/cccss/21/