PROPUESTA DE UNA GUÍA DE SEGURIDAD INFORMÁTICA INTEGRADA A LA GESTIÓN DE LA CALIDAD.

Licenciada. Yamilet Mirabal Sarria.
yamim@eco.upr.edu.cu
Universidad Hermanos Saiz Montes de Oca
Pinar del Río. Cuba
Licenciada. Maria Isabel Maragoto Maragoto.
eniap1@vega.inf.cu
Económica de la Unidad de Investigaciones Aplicadas
Universidad de Pinar del Río. Pinar del Río. Cuba

RESUMEN

Palabras claves: Auditoría informática. Gestión de la Calidad. Seguridad Informática. Tecnología de información.

En el segundo semestre del 2011, la Oficina de Seguridad para las Redes Informáticas, efectuó un control a la Seguridad Informática en el Ministerio de la Construcción en todo el país, a raíz de los resultados de este control se orienta integrar la Seguridad Informática al Sistema de Gestión de las Calidad., conllevando a un reajuste de todos los procedimientos de seguridad informática, como objetivo de esta decisión está un mejor monitoreo, evaluación y control de la actividad informática en las empresas.

Consideramos necesario el uso de una guía de auditoría basada en las normas del Sistema Internacional de Normalización. Comité de Investigación Electrotécnica. Norma No. 17799/2007 sobre las tecnologías de la información, con el objetivo de adaptar el proceso de evaluación de la actividad a su integración al sistema de calidad, proveer sobre todo a los auditores internos de gestión de la calidad de una guía homogenizada que se adapte a lo establecido y evalúe la correcta elaboración e implementación de los procedimientos de seguridad informática.

Con la aplicación de esta guía, se evaluaría no solo el cumplimiento de las políticas de seguridad informática, sino evalúa su objetividad, contribuyendo a una correcta aplicación y orientación a los auditores internos de calidad, sin necesidad de ser especialistas.

Palabras claves: Auditoría informática. Gestión de la Calidad. Seguridad Informática. Tecnología de información.

INTRODUCCION:

La Seguridad Informática establece controles de operación a los sistemas de información desde todas sus aristas, tratando de prevenir y atacar sus vulnerabilidades, teniendo como pilares fundamentales la integridad, disponibilidad y confidencialidad de la información que en ellos se procesa; en tanto la información debe de cumplir con todos los atributos necesarios para considerarse un recurso básico y critico para la organización.

Las acciones generadas por una mala implementación y evaluación de estos controles, pueden estar relacionadas con figuras convencionales tales como: el, desconocimiento, la desorganización, dispersión de criterios, carencia de personal que fiscalice o rectoree la actividad sistemáticamente, sirviendo de contrapartida a los especialistas informáticos y de seguridad informática de la organización. El acto de realizar dichas acciones con el auxilio de medios informáticos precisa, en cada caso, un reanálisis de los elementos de control de la actividad desde dentro de las organizaciones hasta afuera, es decir, un reanálisis de los escasos mecanismos y procedimientos de evaluación de la actividad de informática.

Dentro de las causas que dificulta la gestión de las tecnologías de información dentro de las organizaciones, se puede hablar del excesivo poder de los informáticos dentro de la misma, ya que los sistemas informáticos son, por su naturaleza, un tema esotérico, los técnicos lo saben y han ejercido un tremendo poder debido a su experiencia. También es una realidad que en un gran número de organizaciones el responsable de seguridad informática solamente es un nombre en un papel y no se termina de entender que la seguridad de la información y la seguridad del equipamiento que la respalda es responsabilidad del usuario de esa tecnología y de su jefe inmediato superior; constituyendo un elemento clave dentro de la disciplina laboral y de convivencia.

En nuestro país la seguridad informática está amparada legalmente por la Resolución 127 del 2007 del Ministerio de la Informática y las Comunicaciones, independientemente de su actividad rectora, no es suficiente para implementar una eficiente seguridad pues no propone, normas ni procedimientos a seguir para poder evaluar la misma, tan propensa en esos momentos a hechos delictivos o de corrupción., además se comprobó que es muy difícil evaluar la misma de forma más integral sin un documento que sirva de ayuda y guía para aquella persona que no sea especialista, por su amplitud y especificidades técnicas, para así poder prever a tiempo cualquier situación delictiva.

1. Guía de Auditoría Interna, según lo Establecido en la Norma Cubana ISO/IEC 17799/2007 sobre Tecnología de la Información.

EL hecho de que independientemente los monitoreos y auditorías que se efectúan como parte de las políticas de seguridad, que siempre van a estar sujetos generalmente a los informáticos y responsables de informática, actualmente la empresa cubana no cuenta con auditores internos preparados para evaluar el proceso de seguridad de la información y sus tecnologías, es más, incluso el mismo responsable de seguridad informática, se pierde entre procedimientos, registros y actas, sin la certeza de que realmente no sea vulnerable su sistema.

Lógicamente, ninguna organización cubana es idéntica, ni cuenta con los mismos recursos físicos ni humanos, pero si tiene que proceder de acuerdo a lo legislado en el país, por lo que los temas a revisar serían los mismos, solamente tomando lo que tienen y desechando los servicios que no brindan o con lo que no cuentan.

Cuba, cuenta con varias instituciones cuyo objeto social es supervisar, evaluar y rectorear esta actividad, el desarrollo logístico de estas instituciones no ha ido parejo con el incremento del uso de las tecnologías de la información, independientemente de que son apoyados por otras instituciones que de cierta forma están vinculadas con la actividad de seguridad informática, consideramos deben enriquecerse con personal de experiencia que ayude a asesorar a las organizaciones de forma más sistemática, cuestión esta no debe constituir un problema con las ventajas de nuestro sistema de educación y el desarrollo de las ciencias informáticas en el país, lo que si consideramos un problema es la diversidad de criterios dentro de esas organizaciones, en ocasiones se proponen controles y temas a evaluar de una forma o mediante una metodología determinada y en otro momento se plantea algo totalmente diferente sin llegar a un consenso, esto genera más dudas y duplicidad de trabajo e información, conllevando todo esto en la mayoría de los casos a malestar y apatía a estos tipos de controles.

Concluyendo podemos decir que la actividad de seguridad informática y la integralidad de la gestión de la información en una empresa, es muy amplia y llena de diferentes aristas pudiendo llegar a contar con más de 20 objetivos a controlar.

Consideramos que de contar los auditores internos de la empresas con una guía de auditoría informática lo más integral posible y que toque la mayor cantidad de objetivos, muchas de las situaciones que detectan los compañeros de la

organizaciones externas se pudieran preveer con anterioridad.

1.1 Las Normas ISO y la Seguridad Informática.

Existen innumerables guías para esta actividad, pero todas dirigidas a un punto específico dentro de la misma, para evitar los inconvenientes que pudiera traer ese nivel de especialización para nuestros auditores, consideramos utilizar como base para esta guía a las **normas ISO** las cuales han permitido homologar y consolidar las buenas prácticas, internacionalizar las soluciones y dar cobertura legal a las administraciones más renovadoras, dentro de ellas tenemos a la norma Sistema Internaccional de Normalización. Comité de Investigación Electrotécnica Norma No. 17799/2007 (UNE-ISO/IEC 17799:2007) sobre Tecnología de la Información y código de buenas prácticas para la gestión de la seguridad de la información. Esta norma establece un conjunto de recomendaciones referidas a la política de seguridad, organización de la seguridad de los recursos humanos, seguridad física y ambiental, control de las comunicaciones y de las operaciones, control de acceso y conformidad legal, entre otras; una gran parte de estas recomendaciones se tuvieron en cuenta a la hora de estructurar esta guía, teniendo en cuenta además que estamos certificados por la ISO 9001/2008.

Como ya hemos analizado existen muchas guías de auditorías a las tecnologías de la información, pero todas dependen de lo que se pretenda revisar o analizar, es decir del alcance y objetivo específico, no existe una guía que toque al menos los puntos fundamentales dentro de cada una de las variadas actividades a verificar dentro de las tecnologías de la información,

Es por esto que proponemos una guía única, que permita la implementación y desarrollo de una auditoría a las tecnologías de la información como una herramienta estratégica en la organización, de manera que su aplicación consecuente se convierta en una práctica coherente y continua, que contribuya con la formación de una cultura organizacional de apertura, aprendizaje y mejoramiento progresivo, y a una mayor estabilidad y seguridad integral de la entidad.

La terminología usada en esta propuesta ha sido escogida para que sea congruente y manejable para todos los especialistas de las empresas. Se han evitado aquellas

palabras que tienen diferentes significados y se han reemplazado por palabras que pueden ser entendibles para cualquier trabajador.

Premisas para la aplicación de la guía para las tecnologías de la información:

- Lograr un convencimiento consciente de que la seguridad de la información y la tecnología que la respalda no es responsabilidad de una sola persona, ni de un departamento, es responsabilidad de todos los trabajadores, y que ellos son los responsables de su cumplimiento.
- Capacitar a todos los dirigentes y trabajadores, en función de incrementar la cultura organizacional en el tema de seguridad informática y su integración al sistema de gestión de la calidad.
- Concientización de los ejecutivos a todos los niveles de la empresa, de la importancia de la auditoría como elemento fundamental para la organización, como vía de ayuda, evaluación y control de la actividad.
- Concientizar a los trabajadores de las amenazas de seguridad informática a que se exponen en las funciones que realizan y los efectos que su materialización pueden causar en los resultados de su trabajo.
- Contar con, o formar, el capital humano necesario para implementar todos los diferentes tipos de controles a la información y a la actividad informática.
- Contar con un cuerpo de auditores internos de gestión de calidad que contribuya con su interés y experiencia a una buena interpretación, aplicación y uso de esta guía.

Desde nuestra consideración, y teniendo en cuenta la decisión de integrar la seguridad informática al sistema de gestión de la calidad, así como el empeño de nuestro gobierno en la lucha contra la corrupción y la ilegalidad se hace necesario el uso de una guía de auditoría que unifique criterios tocando todas las aristas la UNE-ISO/IEC 17799:2007. **Ver muestra de la guía de auditoría, Anexo No.1**

Conclusiones

1. La integración de la Seguridad Informática al Sistema de Gestión de la Calidad, es un paso de avance para el buen funcionamiento de la actividad, su

organización y control.

2. Actualmente se hace imprescindible para la actividad de auditoría y de seguridad informática contar con una guía homogénea basada en las normas de gestión de la calidad.
3. Con la Guía de Auditoría propuesta, basada en las Normas ISO, se le suministra a los auditores de gestión de la calidad de las empresas una herramienta eficiente para la revisión, evaluación y control de la actividad informática la que puede llegar a contar con más de 20 objetivos a controlar.
4. Es necesario incrementar los mecanismos de capacitación y divulgación de la importancia del uso de las Normas de Calidad, así como también en la necesidad de concientizar la seguridad informática como un deber a cumplir y controlar por todos.

Bibliografía

1- Amoroso Fernández, Yarina. (2002.) *"El Delito Informático*", Conferencia Magistral Diplomado de Criminalística, Ciudad Habana.
2- *Auditoría y Control, Revista,* (2000).Vol. 1 No. 2, La Habana, Cuba. Edición Especial.
3- *Auditoría y Control, Revista, (*2001) Vol. 1 No. 3, La Habana, Cuba. Edición Especial,
4- *Auditoría y Control, Revista*, (2002) Número 6 La Habana, Cuba.
5- *Auditoría y Control, Revista*, (Diciembre 2002) Número 7 La Habana, Cuba, .
6- Ministerio de la Informática y las Comunicaciones, Resolución 127 del 2007.
7- UNE-ISO/IEC 17799:2007.

Anexo No.1

Guía de control. (Muestra)

Política de seguridad (Resolución 127 del 2007, MIC)	**50 % Muy Mal**	**60 % Mal**	**70% Bien**	**80 % Muy Bien**	**90 % Excelente**
Está establecido en el Plan de Seguridad Informática el compromiso de la Dirección y el enfoque de la organización para gestionar la seguridad de la información.					
Esta definida la seguridad de la información, sus objetivos y alcance generales					
Están determinados los objetivos de control y controles, incluyendo la estructura de la evaluación del riesgo y gestión del riesgo					
El plan de Seguridad Informática cumple con los requisitos legislativos, reguladores y contractuales requisitos de educación, establece los requisitos de formación y concientización en materia de seguridad; tiene establecido los procedimientos de gestión de la información que posibilite de la continuidad del negocio; y las consecuencias de las violaciones a la política de seguridad de la información.					
Están definidas las responsabilidades generales y específicas en materia de gestión de la seguridad informática según lo establecido por la Resolución 127 del 2007 del Ministerio de la Informática y las Comunicaciones.					
El Plan de Seguridad Informática cuenta con las referencias a la documentación que pueda sustentar la políticas de seguridad ; por ejemplo, Procedimiento de Salva de la Información, procedimientos de adquisición e implementación de Software tanto operativos como de aplicación, procedimientos para el mantenimiento y reparación de la tecnología, procedimiento para el traslado de recursos informático y otros que considere necesario la dirección de le empresa, los mismos estarán mucho más detallados para sistemas de información específicos o las reglas de seguridad que los usuarios deberían cumplir.					
Todas estas políticas son del conocimiento de todos los usuarios de la organización y que se les comunica de manera pertinente, accesible y comprensible.					