*Autor: José Torres (jtorres@scientech.com.ve)*
*Director de Tecnología e Información*
*Scientech de Venezuela*
*www.scientech.com.ve*
*Fuente: http://www.pc-news.com/detalle.asp?sid=&id=11&Ida=1245*

# ¿Cómo justificar un proyecto de seguridad informática?

En la actualidad uno de los problemas fundamentales para los lideres y responsables del las unidades de informática de las empresas es lograr obtener recursos para asegurar los activos digitales, seguidamente se exponen las razones fundamentales que justifican la ejecución de un proyecto de consultoría de seguridad informática para la plataforma de cualquier organización. Para la presentación de la información se mostrarán algunos tópicos de la seguridad informática como variables de decisión y su correspondiente situación dentro de cada organización.

_____

El término seguridad tiene múltiples significados según el ambiente donde se utiliza. A efectos de este documento definiremos seguridad informática como el conjunto de reglas, planes y acciones que permiten garantizar la prestación de servicios y asegurar la información contenida en un sistema computacional. El origen de las amenazas es múltiple, desde fenómenos naturales, como un sismo, hasta artificiales como un accidente, espionaje corporativo, sabotaje, desastres causados por virus, ataques cibernéticos, fuga de información o la piratería electrónica.

Según estadísticas internacionales, el número de incidentes de seguridad reportados ha crecido de 2.134 en el año 1997 a 82.094 en el 2002. Para el primer cuatrimestre del año en curso el número de incidentes reportados va por 42.586. Este número de incidentes está distribuido entre todos los países y ninguno escapa a la ocurrencia de los mismos aún cuando aparentemente su desarrollo en el área de la computación sea incipiente. Adicionalmente, pretender cumplir con las metas diarias sin la utilización de los servicios de cómputo disponibles en el mercado para cualquier industria, resultaría imposible, por lo que es imprescindible crecer de forma organizada y segura, así como resguardar la información y servicios existentes.

**Objetivos a alcanzar con la ejecución del proyecto de consultoría en seguridad informática**

Es importante destacar que aun cuando podamos mencionar algunos de los objetivos que alcanzaremos con la ejecución del proyecto, intrínsecamente el simple hecho de incrementar la cultura organizacional respecto a la seguridad informática genera una cantidad de objetivos adicionales que se estarían cumpliendo como consecuencia del desarrollo de una evaluación de seguridad. A continuación se listan algunos de los objetivos fácilmente identificables:

· Evaluar la situación actual de la plataforma tecnológica con respecto a la seguridad informática.
· Identificar las amenazas a las que estamos expuestos.
· Identificar los posibles orígenes de estas amenazas.
· Identificar configuraciones deficientes en los componentes de la plataforma que pudiesen ocasionar fallas o bajo rendimiento.
· Clasificar nuestros recursos tecnológicos en función de su importancia para los niveles estratégicos.
· Evaluar las prácticas de seguridad utilizadas por el personal.

· Evaluar la situación del recurso humano como ente relacionado con la información y la plataforma donde esta reside.
· Identificar el nivel de riesgo que estamos dispuestos a aceptar.
· Identificar las medidas que podemos implantar para proteger los recursos de información en forma económica, eficaz y oportuna.
· Seleccionar las herramientas de seguridad informática necesarias para alcanzar el nivel de seguridad óptimo en las operaciones.
· Realizar las correcciones a las vulnerabilidades detectadas en el proceso de evaluación de seguridad de nuestra plataforma tecnológica.
· Realizar las correcciones asociadas a configuraciones deficientes de los componentes de la plataforma tecnológica.
· Desarrollar y documentar las políticas de seguridad informática, basadas en las mejores normas y prácticas internacionales (ISO 17799).
· Desarrollar un plan de concienciación en seguridad informática para el recurso humano.
· Ejecutar el plan de concienciación en seguridad informática.
· Desarrollar un plan de adiestramiento en los procedimientos del buen uso y mantenimiento de las herramientas de seguridad implantadas en la plataforma tecnológica.
· Ejecutar el plan de adiestramiento en los procedimientos del buen uso y mantenimiento de las herramientas de seguridad para el personal técnico informático.
· Generar recomendaciones dirigidas a mejorar el desempeño de los componentes críticos de la plataforma tecnológica y optimizar sus niveles de seguridad.
· Generar recomendaciones de diseño para la óptima disposición de los elementos en la red.
· Generar guía de mandatos básicos para permitir el crecimiento de la red manteniendo el nivel de seguridad, de acuerdo a las estrategias de negocio a corto, mediano y largo plazo.
· Generar reporte detallado de vulnerabilidades y brechas de seguridad identificadas.
· Generar reportes detallados de correcciones efectuadas a la plataforma.
· Generar reportes en formato ejecutivo que resuma todos los hallazgos obtenidos y las recomendaciones asociadas, que permitan a los niveles estratégicos tomar decisiones inmediatas respecto a la seguridad de su información.
· Mantener durante todo el proceso un programa de apoyo y asesorías al personal técnico informático, por consultoras experimentadas.

**Ventajas**

El desarrollo de este tipo de proyectos en términos generales mejoraría rápida y efectivamente los niveles de calidad en la prestación de los servicios de tecnología ofrecidos por la organización a nuestros clientes internos y externos, no solamente desde el punto de vista de mejora del rendimiento, sino también asegurando la información, su integridad, y confiabilidad y dedicando los recursos para lo que están planificados.

A continuación se listan algunas ventajas específicas que estarían disponibles inmediatamente con el inicio de un proyecto de seguridad informática:

· Mejoras en la disponibilidad de la información.
· Integridad de la información.
· Prestación de servicios tecnológicos de calidad.
· Disminución de problemas operacionales provocados por fallas o anomalías incitadas por incidentes de seguridad (ataques, robos, sabotajes, etc.).

· Transferencia de conocimiento entre el personal técnico informático y expertos especialistas de la seguridad informática.
· Soporte continuo por consultores especialistas durante todo el proceso de evaluación, corrección y adiestramiento.
· Drástica reducción de costos asociados a pérdidas de información por incidentes de seguridad.
· Evitar la manipulación de información confidencial por personas no autorizadas (internas o externas).
· Incremento del nivel de concienciación del personal con respecto a los tópicos de seguridad informática.
· Aumento de las destrezas en técnicas asociadas con la detección, prevención y corrección de incidentes que amenacen los activos de la organización.
· Reducción de los tiempos de evaluación e implantación de soluciones indispensables de seguridad informática.
· Reducción en los costos asociados a adiestramiento y formación del personal técnico especializado en seguridad informática.
· Reducción de tiempos de dedicación del recurso humano en la ejecución de actividades especializadas.
· Atención de consultores dedicada al desarrollo de actividades del proyecto con planificación anticipada.

**Costo/Beneficios**

Los costos asociados a problemas de seguridad son múltiples y variados. En esta sección definiremos algunos y haremos referencia a los beneficios que obtendremos con la ejecución de un proyecto de seguridad informática.

Uno de los principales problemas que afrontamos diariamente en nuestras organizaciones es la inexistencia de una política de seguridad informática corporativa bien definida y documentada, este documento representa la base que soporta cualquier esfuerzo dirigido a mejorar el nivel de la plataforma con respecto a su seguridad informática. Entonces, este es el punto de partida para cualquier iniciativa al respecto, pero ¿Cómo aplicar políticas sin una evaluación profunda de la situación de la plataforma, las herramientas que soportan la información, la determinación del nivel de conciencia de nuestros usuarios, sin conocer realmente que activo de información es más importante proteger o resguardar para la organización. De allí que solo podemos mencionar que constantemente estamos dedicando inversiones dirigidas a la mejora de nuestra plataforma, de equipos prestadores de servicio, componentes responsables del procesamiento de la información, estaciones de trabajo y sus aplicaciones, la pregunta es ¿Cuál es el valor de esta plataforma?, ¿Estamos interesados en poner la información e inclusive nuestros servicios, fácilmente accesibles por terceros no autorizados o solo a quienes nosotros decidimos, a quienes nuestras políticas imponen?, así, parece imperante conocer ¿A que riesgo nos enfrentamos?, ¿Con que herramientas contamos?, ¿Qué tan eficientes son? y ¿Qué especialistas están disponibles para afrontar cualquier situación?.

En términos generales, ¿Qué inversión será necesaria para disponer de un equipo de especialistas en seguridad informática?, ¿Estamos dispuestos a soportar el tiempo y los riesgo que a ciencia cierta desconocemos y nos asechan?, ¿Cuántas herramientas de análisis y evaluación de plataformas de seguridad serian necesarias adquirir para tener una somera visión de nuestra seguridad?, ¿Cuántos recursos perdemos diariamente?, y finalmente, ¿Cuánto nos costaría formar un equipo de

especialistas altamente adiestrados en cada una de las áreas relacionadas con el proyecto?.

Definitivamente la labor es compleja y la responsabilidad inmensa, asegurar nuestra información es una actividad continua y necesaria.