Seguridad opcional, seguridad integral

Enero 2006

Agustín López

Ing. Informático

Lead Auditor BS7799 certificado por BSI

www.iso27000.es

En éste artículo analizamos los enfoques básicos empleados por las organizaciones a la hora de afrontar la gestión de la seguridad de su información.

Dentro del concepto de “la seguridad como opción” se podrán reconocer un número importante de empresas a las que recomendamos consideren la adopción de modelos integrados como la vía más racional en seguridad.

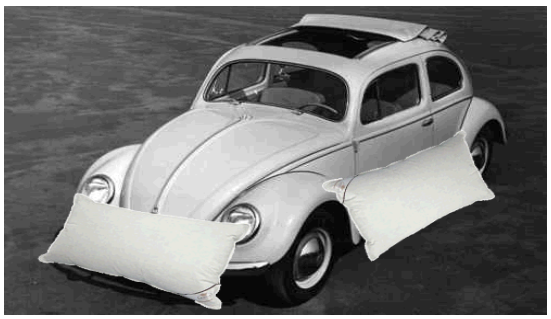
Especialmente, en aquellas organizaciones que dedican grandes esfuerzos en el desarrollo y mantenimiento de estructuras propias para la regulación y auditoria de sus niveles de seguridad y que podrán encontrar en el estándar ISO 27000 una fuente de ahorro considerable en los recursos y esfuerzos dedicados, mediante la adopción del estándar e independientemente de la decisión final de certificarse en el estándar ISO 27001.

La seguridad como opción

Cuando la seguridad supone un reto de integración, un gasto sin un retorno evaluable de la inversión y se considera posteriormente al desarrollo e implantación de procesos conocidos en la organización, significa entonces, que es considerado un “añadido” que trata de proporcionar protección a los procesos e información de manera independiente.

Este modelo de gestión de la seguridad suele ser consecuencia de un rápido desarrollo tecnológico dentro de la organización sin una adecuada actualización simultánea de las políticas internas en relación a los nuevos medios técnicos de acceso a la información implantados.

De éste modo, si antes la información susceptible de ser tratada como confidencial se guardaba celosamente en papel y bajo un determinado número controlado de llaves autorizadas, cuando la misma información pasa al formato de ficheros almacenados en servidores, sigue protegida mediante una puerta de acceso aunque hayan aumentado las vías para el acceso, duplicación o manipulación por redes LAN o WAN, MODEM administrativos o copias de respaldo.



Al finalizar cada implantación técnica, las medidas en seguridad se añaden en la organización rápidamente y a medida que se hacen evidentes las violaciones en la confidencialidad, integridad y disponibilidad de la información, asumiendo niveles de riesgo inciertos de paradas o retrasos en los procesos críticos de negocio al no existir un proceso establecido para su evaluación.

La introducción de soluciones rápidas que garanticen la recuperación y continuidad de negocio en éstas condiciones supone, con mayor frecuencia de la esperada, desequilibrios en las previsiones económicas que se deben compensar internamente y en el aspecto técnico, entornos complejos para la integración de sistemas difíciles de gestionar y mantener.

Las deficiencias en la reorganización de políticas, asimilación de tareas y/o formación de responsables y usuarios conducen a la recuperación y pérdida continuada del control efectivo de la seguridad.

La seguridad integral

La seguridad de la información es gestionada de modo integrado cuando, es considerado en el desarrollo y mantenimiento de los procesos de la organización, las medidas implantadas a modo de controles pueden aplicarse y extenderse a más de un proceso o función y existe un modelo de inversión establecido y evaluable que es acometido junto al resto de cuestiones económicas de primer orden por parte de los órganos de dirección.

Mediante políticas que cuentan con el apoyo de la dirección y son efectivamente aplicadas a lo largo de toda la organización, la seguridad es adaptada del mejor modo a la dinámica del cambio continuo interno y del entorno y se aprovecha del modo más eficiente posible en relación a las inversiones realizadas.

Las organizaciones que consideran seriamente la seguridad de su información conocen las limitaciones de los controles independientes de carácter exclusivamente técnico y la necesidad fundamental de la acción combinada de las personas junto a la implantación racional de controles relacionados a procesos e información claves dentro de la organización.

Considerando que los presupuestos dedicados a la seguridad deben ser racionalmente limitados pero las necesidades en implantación de medidas preventivas y controles tienden a aumentar, se hace necesario dirigir las inversiones allí donde la protección demuestre ser más necesaria en cada momento.

Las evidencias para éste propósito se logran mediante un proceso comprensible y reproducible de análisis de riesgos, en el que las amenazas y vulnerabilidades, que pueden afectar a los activos de información de la organización, se analizan y resuelven mediante la implantación y reconfiguración de unos controles de seguridad viables, efectivos y sostenibles por los presupuestos dedicados a lo largo del tiempo.

ISO 27000, como estándar efectivo para la gestión de la seguridad de la información de ámbito internacional, es un medio adecuado y reconocido para lograr que la seguridad pase a estar perfectamente integrada en los procesos de negocio y aporte los beneficios esperados para las empresas mediante una mejora continuada, demostrable y evidente de la seguridad de la información en toda la organización.