Servicio: Asesoría para la elaboración del Sistema de Gestión de la Seguridad Informática

Precio: CUP: $49968.00

Exportable: No
Calificación: 0.0
Comentarios: 0
Vistas: 424

Descripción:

Antes de abordar un enfoque metodológico para implementar un SGSI es necesario aclarar la diferencia entre seguridad informática y seguridad de la información, la cual radica en el tipo de recursos sobre los que actúa cada una. Mientras que la primera se enfoca en la tecnología propiamente dicha, i.e. en las infraestructuras tecnológicas que sirven para la gestión de la información en una organización, la segunda está relacionada con la información en sí misma, como activo estratégico de la organización. En este sentido las TIC son herramientas que permiten optimizar los procesos de gestión de la información en las organizaciones. El concepto de seguridad es el mismo, pero mientras la seguridad informática desarrolla su función sobre todos los elementos técnicos que hacen parte de las TIC, la seguridad de la información actúa sobre la información como activo estratégico para la adecuada toma de decisiones empresariales en las organizaciones modernas.

Características:

Plan de Prevención de Riesgos

La gestión de riesgos persigue la disminución de las probabilidades de los impactos negativos en un proyecto o en determinada actividad de la empresa y, al contrario, busca aumentar las probabilidades de que se produzcan impactos positivos en esas actividades.

Plan de Contingencias

Surge de un análisis de riesgos, donde entre otras amenazas, se identifican aquellas que afectan a la continuidad de la operación de la entidad. El plan de contingencias deberá ser revisado semestralmente, así mismo, es revisado/evaluado cuando se materializa una amenaza. El plan de contingencia tiene en cuenta las amenazas y vulnerabilidades a las que están expuestas las tecnologías informáticas de la entidad

Estudio de Vulnerabilidades

Las necesidades y prioridades de protección de los diferentes activos tecnologicos de la entidad se determinan mediante la realización del Análisis de Riesgos, que es el proceso dirigido a determinar la probabilidad de que las amenazas se materialicen sobre los bienes informáticos, e implica la identificación de los bienes a proteger, las amenazas que actúan sobre ellos, su probabilidad de ocurrencia y el impacto que puedan causar.

Plan de Seguridad Informatica

El desarrollo del PSI como materialización documentada de la recolección técnica y general de información ya indicada anteriormente, persigue un doble objetivo. Por una parte conformar una documentación que recoja de forma concisa y clara el estado, tanto técnico como organizativo, de la organización en el campo de la seguridad informatica de la entidad, lo que en sí mismo, suponga un activo importante para la organización que pueda ser utilizado, en adelante, como documentación de referencia que regule y establezca las normas y procedimientos a cumplir en materia de seguridad de sistemas y seguridad de la informacion en la entidad.

Manual de Procedimientos

Un Manual de Procedimientos tiene como propósito operar como instrumento de trabajo para el cumplimiento de lo establecido en basamento legal para la actividad informática y todo lo que a ella se refiera en otros temas como el control interno, procedimientos que servirán de guía y apoyo para el control y uso seguro por los usuarios de los servicios informáticos, en los cuales se recogen los procesos de mayor impacto dentro de la informática, el software y los servicios que se brindan en a entidad