

CONCEPTOS BÁSICOS (SEGURIDAD INFORMÁTICA)

SEGURIDAD INFORMÁTICA

Hoy en día la seguridad informática se ha convertido en una de las principales preocupaciones de las empresas. Por otro lado el uso de las tecnologías de la información y comunicaciones (TIC), es cada vez más extenso por lo que los activos a proteger y las vulnerabilidades aumentan; y por otro lado los ciberataques son más frecuentes y complejos, llegando a tener consecuencias muy graves como la revelación de información entre otras, por lo que disponer de profesionales en seguridad TIC que puedan proteger los activos en la red se hace imprescindible en todas las empresas por pequeñas o grandes que estas sean.

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. También se ocupa de diseñar los procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.

Para lograr sus objetivos la seguridad informática se fundamenta en tres principios, que debe cumplir todo sistema informático:

Confidencialidad: Se refiere a la privacidad de la información almacenada y procesada en un sistema informático, las herramientas de seguridad informática deben proteger el sistema de intrusos y accesos por parte de personas o programas no autorizados. Este principio es importante en aquellos sistemas en los que los usuarios, computadoras y datos residen en lugares diferentes, pero están física y lógicamente interconectados.

Integridad: Se refiere a la validez y consistencia de los elementos de información almacenados y procesador en un sistema informático. Basándose en este principio, las herramientas de seguridad deben asegurar que los procesos de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es importante en aquellos sistemas en los que diferentes usuarios, computadoras y procesos comparten la misma información.

Disponibilidad: Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran.

Los invito a revisar algunas de las acciones que las empresas deben tomar en cuenta para una mejor seguridad:

- Crear e implementar una estrategia de seguridad completa – desde la predicción de posibles peligros y riesgos a la Prevención de las amenazas en curso, todo ello apoyado por detección y una respuesta eficaz.
- La ciberseguridad es demasiado compleja y grave para mezclarla con generalidades TI. Se debería considerar la creación de un Centro de Operaciones de Seguridad dedicada.