Fundamentos de la Gestión de Incidentes

La gestión de incidentes existe como consecuencia de la gestión de la seguridad. ES el proceso para detectar, reportar, valorar, respoder a, tratar con y responder a los incidentes de seguridad. Hay que ser capaz de ver que se está sufriendo un incidente y actuar para eliminarlo o reducirlo. La parte más importante es aprender de los incidentes para saber como reaccionar a futuro o crear contramedidas para estos incidentes. El objetivo es ver que todos los eventos de seguridad e identificar si son maliciosos o no. La gestión de incidentes tiene un enfoque reactivo para manejar incidentes de seguridad.

CSIRT vs CERT

- CSIRT: Equipo de respuestas a incidentes de seguridad en computadores (Mercado Europeo)
- CERT: Equipo de respuesta a incidentes en computadores (Mercado Estadounidense)

From:
https://knoppia.net/ - **Knoppia**

Permanent link:
https://knoppia.net/doku.php?id=master_cs:gsi:ginc&rev=1761586158

Last update: **2025/10/27 17:29**