

Un incidente è definito come un evento che può avere effetti negativi sulle operazioni del sistema e che si può configurare come frode, danno, abuso, compromissione dell'informazione, perdita di beni.

La gestione degli incidenti è strettamente legata alla pianificazione delle eventualità critiche.

La struttura di gestione degli incidenti deve essere considerata una componente della pianificazione, poiché garantisce la possibilità di rispondere rapidamente ed efficientemente all'evento negativo e di portare a termine le normali operazioni in seguito a danneggiamento.

Occorre prevedere:

- Contenimento e riparazione del danno derivante dagli incidenti.
- Prevenzione dei danni futuri.
- Benefici collaterali.

I membri del gruppo di gestione degli incidenti devono avere le opportune conoscenze e capacità, sia di tipo tecnico che non tecnico, che sono:

- Familiarità con la tecnologia cui si rivolge la struttura di gestione degli incidenti.
- Abitudine a lavorare in un gruppo.
- Abitudine a comunicare in maniera efficace con diversi tipi di utenti, che vanno dall'amministratore di sistema agli utenti inesperti ed ai dirigenti.
- Disponibilità ad intervenire ventiquattro ore su ventiquattro.
- Possibilità di spostamenti rapidi.

È estremamente importante imparare a rispondere in maniera efficace ad un incidente. Le ragioni principali sono:

- Evitare danni diretti alle persone.
- Evitare danni economici: se il personale che deve rispondere ad un incidente è stato adeguatamente istruito, il tempo richiesto a queste persone per gestire l'incidente è ragionevolmente limitato e possono essere utilizzate in altri ambiti.
- Proteggere informazione classificata, sensibile o proprietaria: uno dei danni maggiori di un incidente alla sicurezza è che l'informazione potrebbe rivelarsi irrecuperabile. Un'opportuna gestione degli incidenti minimizza questo pericolo.