- Limitare i danni all'immagine dell'organizzazione: le notizie sugli incidenti di sicurezza tendono a danneggiare il rapporto di fiducia tra un'organizzazione, le persone, le altre organizzazioni e l'opinione pubblica.

È importante stabilire con anticipo la priorità delle azioni da compiere durante un incidente. A volte un incidente può essere troppo complesso da fronteggiare in modo globale e simultaneo in tutte le sue implicazioni quindi é essenziale stabilire le priorità:

Priorità 1: proteggere la sicurezza delle persone

Priorità 2: proteggere i dati classificati o sensibili

Priorità 3: proteggere gli altri dati, inclusi i dati scientifici, proprietari e relativi alla gestione

Priorità 4: prevenire i danni al sistema

Priorità 5: minimizzare i danni alle risorse tecnologiche ed elaborative.

Chi deve essere avvertito

Il personale tecnico, gli Amministratori, i gruppi di risposta, le forze di polizia, i fornitori e distributori del software, altri fornitori di servizio. In casi specifici e preventivamente individuati, può essere anche necessario informare la stampa e/o la comunità degli utenti ed altre organizzazioni che potrebbero essere vittime dello stesso tipo di incidente.

Chi deve essere coinvolto

Per la gestione degli incidenti, deve essere creato un gruppo di risposta agli incidenti formato da Tecnici specialisti delle varie Aree Tecnologiche e da Esperti funzionali dell'Amministrazione.

Risposta all'incidente

La risposta ad un incidente si svolge attraverso le fasi di contenimento, di eliminazione, di ripristino e di azione successiva all'incidente.

Le procedure per trattare questo tipo di problema devono essere chiaramente formalizzate e comunicate. Occorre prevedere:

- Chi ha l'autorità di decidere quali azioni intraprendere
- In che momento e se devono essere coinvolte le forze di polizia