

## ALLEGATO I

**REQUISITI E COMPITI DI GRUPPI DI INTERVENTO PER LA SICUREZZA INFORMATICA IN CASO DI INCIDENTE (CSIRT)**

I requisiti e i compiti dei CSIRT sono adeguatamente e chiaramente definiti nel quadro di una strategia e/o di una regolamentazione nazionale. Essi includono quanto segue:

## 1) Requisiti per i CSIRT

- a) I CSIRT garantiscono un alto livello di disponibilità dei propri servizi di comunicazione, evitando singoli punti di guasto, e dispongono di vari mezzi che permettono loro di essere contattati e di contattare altri in qualsiasi momento. Inoltre, i canali di comunicazione sono chiaramente specificati e ben noti alla loro base di utenti e ai partner con cui collaborano.
- b) I locali dei CSIRT e i sistemi informativi di supporto sono ubicati in siti sicuri.
- c) Continuità operativa:
  - i) i CSIRT sono dotati di un sistema adeguato di gestione e inoltro delle richieste in modo da facilitare i passaggi;
  - ii) i CSIRT dispongono di personale sufficiente per garantirne l'operatività 24 ore su 24;
  - iii) i CSIRT operano in base a un'infrastruttura di cui è garantita la continuità. A tal fine è necessario che siano disponibili sistemi ridondanti e spazi di lavoro di backup.
- d) I CSIRT hanno la possibilità, se lo desiderano, di partecipare a reti di cooperazione internazionale.

## 2) Compiti dei CSIRT

- a) I compiti dei CSIRT comprendono almeno:
  - i) monitoraggio degli incidenti a livello nazionale;
  - ii) emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti;
  - iii) intervento in caso di incidente;
  - iv) analisi dinamica dei rischi e degli incidenti, nonché sensibilizzazione situazionale;
  - v) partecipazione alla rete dei CSIRT;
- b) i CSIRT stabiliscono relazioni di cooperazione con il settore privato;
- c) per facilitare la cooperazione, i CSIRT promuovono l'adozione e l'uso di prassi comuni o standardizzate nei seguenti settori:
  - i) procedure di trattamento degli incidenti e dei rischi;
  - ii) sistemi di classificazione degli incidenti, dei rischi e delle informazioni.

---