Confidenzialità dei dati

garantire che i dati e le risorse siano preservati dal possibile utilizzo o accesso da parte di soggetti non autorizzati. La confidenzialità deve essere assicurata lungo tutte le fasi di vita del dato, a partire dal suo immagazzinamento, durante il suo utilizzo o il suo transito lungo una rete di connessione.

Integrità dei dati

la capacità di mantenere la veridicità dei dati e delle risorse e garantire che non siano in alcun modo modificate o cancellate, se non ad opera di soggetti autorizzati. Parlare di integrità significa prendere in considerazione differenti scenari: prevenire modifiche non autorizzate a informazioni da parte degli utenti, ma anche garantire che le informazioni stesse siano univocamente identificabili e verificabili.

Disponibilità dei dati

si riferisce alla possibilità, per i soggetti autorizzati, di poter accedere alle risorse di cui hanno bisogno per un tempo stabilito e in modo ininterrotto. Rendere un servizio disponibile significa impedire che durante l'intervallo di tempo definito avvengano interruzioni di servizio e garantire che le risorse infrastrutturali siano pronte per la corretta erogazione di quanto richiesto.

Le minacce che mettono a rischio la disponibilità di un servizio possono riguardare errori software, rotture di device, fattori ambientali ed eventi catastrofici che mettono fuorigioco le infrastrutture, come interruzioni dell'erogazione dell'energia elettrica, inondazioni, terremoti o Denial of Service/Distributed Denial of Service, interruzioni di comunicazione.

Tutelare la confidenzialità di un sistema informatico

Ci sono migliorie applicabili per garantire la confidenzialità delle informazioni:

- l'utilizzo di software criptati per le comunicazioni fra i dipendenti e la condivisione di file, maggiori fattori di autenticazione, utilizzo di VPN e autenticazione multi fattore, nonché un corso per l'awareness del personale alla sicurezza informatica.

Per migliorare la triade CIA è necessario mettere in atto policy di autenticazione e monitorare l'effettivo accesso e utilizzo delle risorse, con, ad esempio, log.

Sistemi per l'Intrusion Detection, restrizioni di accesso e formazione degli utenti per rispettare questo principio.

sistemi firewall in grado di proteggere le reti interne e sistemi di monitoraggio continuo del traffico

generare password sicure attraverso software appositi.

Devono essere messi in atto meccanismi in grado di mantenere i livelli di servizio definiti, avvalendosi di strumenti di Disaster Recovery, back up e Business Continuity, in grado di limitare gli effetti di possibili indisponibilità di servizio o perdita di dati.