POLITICHE DI SICUREZZA

Tutte le sezioni successive contengono la descrizione per ognuna delle politiche.

1.1 Politica di gestione della sicurezza dei sistemi

La gestione in sicurezza delle infrastrutture informatiche ha l'obiettivo di garantire che i sistemi, le postazioni di lavoro, le applicazioni, i servizi di rete, i servizi elaborativi forniscano le prestazioni elaborative ai livelli e con i requisiti di sicurezza definiti.

Vengono inoltre di seguito sintetizzati i principi generali in base ai quali porre in essere la gestione sicura dei sistemi:

- deve essere gestito ed aggiornato un inventario degli asset hardware e software;
- devono essere applicate regole standard per la installazione e la configurazione dei sistemi;
- le configurazioni dei sistemi devono essere disegnate tenendo in considerazione le esigenze attuali e future delle prestazioni;
- le configurazioni dei sistemi devono indirizzare nel modo più compiuto possibile la sicurezza built-in e devono facilitare l'installazione di ulteriori misure di sicurezza;
- devono essere adottate procedure standard di configurazione dei sistemi che indirizzino:
    - disabilitazione o restrizione nell'utilizzo di alcuni particolari servizi;
    - restrizioni nell'accesso ad utilities di sistema particolarmente critiche ed a funzioni di setting di sistema;
    - utilizzo di funzioni di time-out;
    - le principali esigenze di aggiornamenti in termini di patch e di fix di sicurezza;
- le configurazioni dei sistemi devono essere archiviate ed aggiornate all'interno di un repository governato centralmente;
- devono essere condotte regolarmente attività di monitoraggio sulle prestazioni dei sistemi al fine di gestire adeguatamente eventi, problemi e incidenti.

E' inoltre fondamentale predisporre un'adeguata politica di backup, anche remoto, che naturalmente sia in accordo e coerenza con quanto previsto dal manuale della conservazione.

1.2 Politica per il controllo degli accessi fisici

Descrizione delle modalità di controllo degli accessi fisici, che prevedano, almeno le seguenti classi di accesso:

- personale dell'organizzazione;
- personale di fornitori esterni;
- personale della/delle amministrazione/amministrazioni servite dal sistema di conservazione;
- personale delegato dall'organizzazione (a esempio personale che esegue manutenzione/riparazione, ecc.).

1.3 Politica per l'inserimento dell'utenza e per il controllo degli accessi logici

Descrizione delle modalità di inserimento dell'utenza e attribuzione delle autorizzazioni per gli accessi a sistemi, applicazioni e applicativi dell'organizzazione; comprende anche le modalità di cancellazione o di cambio di autorizzazione, con specifico riferimento al sistema di conservazione documentale.

1.4 Politica di gestione delle postazioni di lavoro

Gli elementi essenziali di questa politica sono:

- provisioning delle postazioni di lavoro;
- regole per l'installazione del software sulle postazioni di lavoro;
- regole per gli aggiornamenti;
- regole per la limitazione della connettività a supporti esterni (CD/DVD, Pen Drive, ecc.);
- regole per la modifica delle impostazioni.

1.5 Politica di gestione dei contenuti applicativi

Descrizione delle attività riguardo la manutenzione dei sistemi, il controllo sul contenuto software dei client al fine di verificare l'assenza di codice malevolo e la conformità a quanto autorizzato e previsto dalle licenze d'uso.

1.6 Politica di gestione, dismissione e smaltimento degli apparati mobili e dei supporti

Particolare attenzione deve essere posta alla gestione degli apparati mobili (portatili, tablet, smartphone, cellulari, ecc.) e dei supporti esterni ai server e alle postazioni di lavoro quali, a esempio: HD esterni/CD/DVD/Pen Drive/DAT/LTO, ecc., ma anche carta stampata, che siano utilizzati e/o prodotti nell'ambito delle attività di conservazione documentale.

La politica regola, oltre che le modalità di utilizzo e conservazione dei dispositivi, anche quelle per la dismissione/distruzione degli apparati e dei supporti.

1.7 Politica di gestione dei canali di comunicazione

I canali di comunicazione, quali e-mail, internet, fax, scanner, fotocopiatrici devono essere controllati al fine di preservare la confidenzialità, e l'integrità delle informazioni in transito, ed allo stesso tempo ad impedire l'abuso che si potrebbe fare di tali strumenti di comunicazione. Di conseguenza la tipologia di controlli deve coprire le problematiche di utilizzo appropriato dello strumento, le problematiche di comportamento dell'utilizzatore dello strumento e le tecnologie coinvolte.

1.8 Manutenzione delle politiche di sicurezza

Deve essere previsto il perfezionamento, la divulgazione e il riesame delle politiche di sicurezza al verificarsi dei seguenti casi:

- incidenti di sicurezza;
- variazioni tecnologiche significative;
- modifiche all'architettura informatica;
- aggiornamenti delle prescrizioni normative;
- risultati delle eventuali attività di audit interni.