Misure di sicurezza e protezione dei dati personali

Queste sono le misure di sicurezza adottate per garantire un livello di sicurezza adeguato al rischio sul sistema SIBAR:

- aggiornamento semestrale dell'inventario hardware, software e delle interfacce di tutti gli applicativi;
- backup giornaliero di tutti gli applicativi e relative basi dati con test periodici con cadenza almeno semestrale dell'efficacia dei backup effettuati e definizione delle procedure di ripristino prestabilite per ciascun applicativo;
- attivazione di un Security Information and Event Management (SIEM) utilizzato per la produzione e consultazione dei log sui sistemi per la prevenzione e il monitoraggio delle intrusioni;
- tutti gli accessi alle macchine virtuali e fisiche sulle quali sono installati gli applicativi sono possibili solo da parte di amministratori di sistema opportunamente nominati, con utenze nominative e non condivise;
- nessun dato dell'ambiente di produzione può essere riversato negli ambienti di pre-produzione, test e/o sviluppo senza l'esplicito consenso scritto da parte del Titolare. Qualora, per esigenze legate al Titolare stesso, quanto sopra fosse effettuato, la permanenza del dato sugli ambienti non produttivi sarà limitata ad un tempo strettamente necessario alle verifiche da parte del Titolare e poi dovrà essere immediatamente cancellato tramite sovrascrittura della base dati da altro ambiente;
- l'accesso a tutti gli applicativi avviene solo tramite Rete Telematica Regionale (RTR) o VPN fornita dal Titolare. Nessun servizio è raggiungibile al di fuori delle Rete Regionale o della VPN suddette;
- l'autenticazione degli amministratori di sistema del vCenter, possibile solo dall'interno della rete regionale o tramite VPN, avviene sulla base di utenze di dominio (RS) di tipo personale;
- l'accesso ai sistemi avviene tramite un software di access manager, l'Oracle Access Manager, che gestisce il single sign on delle utenze. Le password su tale software sono cifrate con un algoritmo standard (SHA-512 - salted). È presente un blocco delle credenziali dopo 8 tentativi di accesso errati;
- tutti i servizi esposti dalle applicazioni utilizzano il protocollo di comunicazione https.

Manuale di gestione documentale della Regione Autonoma della Sardegna - Allegato n. 11