ALLEGATO *D*

“MISURE DI SICUREZZA”

L’infrastruttura di sicurezza a supporto del sistema ANIS deve garantire:

- l’integrità e la riservatezza dei dati;
- la sicurezza dei servizi e dell’accesso ad essi;
- il tracciamento delle operazioni effettuate.

1. Integrità e riservatezza dei dati

L’integrità (la protezione dei dati e delle informazioni nei confronti delle modifiche del contenuto, che siano accidentali oppure effettuate volontariamente da una terza parte) e la riservatezza dei dati presenti nelle banche dati sono garantite da opportune regole di profilazione e secondo il principio dei minimi privilegi necessari. Tutti gli accessi inoltre sono tracciati e registrati in file di *log*.

Per i soli dati necessari ai servizi di monitoraggio, definiti nell’Allegato C, la riservatezza è garantita attraverso l’adozione di misure di anonimizzazione tramite la rimozione dei dati identificativi dell’interessato (Codice Fiscale e, ove presente, ID ANPR) e la memorizzazione in una sezione segregata e distinta della base dati ANIS.

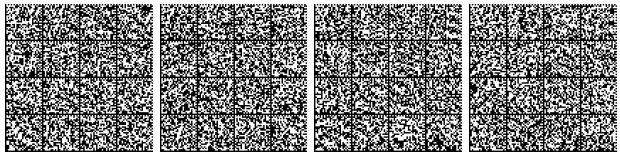
Nel caso di servizi fruiti tramite il Portale ANIS, il non ripudio (condizione secondo la quale non si può negare la paternità e la validità del dato) è garantito sia dalla non modificabilità dei *log* di tracciamento, sia dall’identificazione certa dell’utente da parte del sistema informatico, mediante un meccanismo di autenticazione forte (metodo di autenticazione basato sull’utilizzo di più di un fattore di autenticazione) per l’accesso ai servizi. L’integrità e il non ripudio dei documenti scaricabili dal Portale ANIS sono garantiti attraverso l’apposizione di un sigillo elettronico ad ogni documento.

Per la fruizione dei servizi resi fruibili dalla PDND l’integrità e il non ripudio sono garantiti dalle policy proprie della PDND.

2. Sicurezza dei servizi e dell’accesso ad essi

Per proteggere i sistemi dagli attacchi informatici al fine di eliminare le vulnerabilità, sono rispettate le seguenti tecnologie e/o procedure:

a) aggiornamenti periodici dei sistemi operativi e dei *software* di sistema e *hardening* delle macchine;



b) adozione di una infrastruttura di sistemi *firewall* e sistemi IPS (*Intrusion Prevention System*), che consentono la rilevazione dell'esecuzione di codice non previsto nonché di azioni in tempo reale quali il blocco del traffico proveniente da un indirizzo IP attaccante;

c) esecuzione di WAPT (*Web Application Penetration Test*), per la verifica della presenza di eventuali vulnerabilità sul codice sorgente;

d) adozione di meccanismi, tipo *captcha*, sul Portale ANIS e di sistemi di *rate-limit* (limitanti il numero di transazioni nell'unità di tempo), al fine di mitigare il rischio di accesso automatizzato alle applicazioni, che genererebbe un traffico finalizzato alla saturazione dei sistemi e quindi al successivo blocco del servizio;

e) presenza di sistemi di *backup* e *disaster recovery.* Il backup dovrà riguardare i seguenti elementi: dati, configurazioni dei sistemi, software applicativo, file di log e di alert.

3. Tracciamento delle operazioni effettuate

È previsto un sistema di *log analysis* per l'analisi periodica delle informazioni registrate degli accessi applicativi, tale da individuare, sulla base di regole predefinite e formalizzate e attraverso l'utilizzo di indicatori di anomalie (*alert*), eventi potenzialmente anomali che possano configurare trattamenti illeciti.

I file di *log* registrano le informazioni riguardanti le operazioni per la verifica della correttezza e legittimità del trattamento dei dati, presentando le caratteristiche di integrità e inalterabilità, ed essendo protetti attraverso idonee misure contro ogni uso improprio.

Sono registrati anche i file di *log* relativi agli accessi e alle operazioni effettuate sulle basi dati, nonché i *log* di servizio.

Sulla base di quanto monitorato dal sistema di *log analysis*, devono essere generati periodicamente dei report sintetici sullo stato di sicurezza del sistema (es. accessi ai dati, rilevamento delle anomalie, etc.).

23A00212