ALLEGATO TECNICO

«*Principali garanzie e misure di sicurezza*»

1. Introduzione

Il presente Allegato Tecnico descrive le principali garanzie e misure di sicurezza adottate per garantire la protezione dei dati personali trattati nell'ambito della Sezione ITS dell'ANIST.

I requisiti di sicurezza adottati garantiscono l'integrità e la riservatezza dei dati, la sicurezza dei servizi, il tracciamento delle operazioni effettuate, nonché il rispetto dei principi di protezione dei dati per impostazione predefinita e per progettazione.

Per le predette finalità, la Sezione ITS è dotata di:

a) un sistema di Identity & Access Management per l'identificazione dell'utente e della postazione, la gestione dei profili autorizzativi, la verifica dei diritti di accesso, il tracciamento delle operazioni;

b) un sistema di tracciamento e di conservazione dei dati di accesso alle componenti applicative e di sistema;

c) sistemi di sicurezza per la protezione delle informazioni e dei servizi erogati dalla base dati;

d) un sistema di *log analysis* per l'analisi periodica dei file di log, in grado di individuare, sulla base di regole predefinite e formalizzate, eventi potenzialmente anomali e di segnalarli al Ministero dell'Istruzione e del Merito tramite funzionalità di alert;

e) una Certification Authority;

f) sistemi e servizi di backup per il salvataggio dei dati e delle applicazioni;

g) sistemi e servizi di Disaster Recovery.

Il piano di continuità operativa espliciterà le procedure relative ai sistemi e ai servizi di backup e di Disaster Recovery.

2. Infrastruttura fisica

L'infrastruttura della Sezione ITS dell'ANIST è installata nei locali individuati dal Ministero dell'Istruzione e del Merito aventi specifici requisiti di sicurezza che garantiscano la continuità di servizio tramite soluzioni di alta affidabilità (HA) e un rigido controllo dell'accesso anche fisico in ambienti ad accesso limitato e sottoposti a videosorveglianza continua.

Qualsiasi altra operazione manuale è consentita solo a personale autorizzato dal Ministero dell'Istruzione e del Merito.

3. Protezione da attacchi informatici

Al fine di protezione dei sistemi operativi da attacchi informatici, eliminando le vulnerabilità, si utilizzano:

a) in fase di configurazione, procedure di *hardening* finalizzate a limitare l'operatività alle sole funzionalità necessarie per il corretto funzionamento dei servizi;

b) in fase di messa in esercizio, oltre che ad intervalli prefissati o in presenza di eventi significativi, processi di *vulnerability assessment and mitigation* nei *software* utilizzati e nelle applicazioni dei sistemi operativi;

c) piattaforma di sistemi *firewall* e sonde anti-intrusione;

d) ogni altra soluzione tecnologica aggiuntiva che sia utile all'innalzamento del livello di sicurezza e protezione del sistema.

Per proteggere i sistemi dagli attacchi informatici è adottata una procedura di gestione degli incidenti informatici e sono, inoltre, 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 ANIST 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.

4. Accesso

L'accesso alla Sezione ITS dell'ANIST avviene in condizioni di pieno isolamento operativo e di esclusività, in conformità ai principi di protezione, disponibilità, accessibilità, integrità e riservatezza dei dati, nonché di continuità operativa dei sistemi e delle infrastrutture di cui all'articolo 51 del CAD.

I sistemi di sicurezza garantiscono che l'infrastruttura di produzione sia logicamente distinta da altre infrastrutture, anche di competenza di soggetti terzi di cui il Ministero dell'Istruzione e del Merito si avvalga e che l'accesso alla stessa avvenga in modo sicuro, controllato e costantemente tracciato, esclusivamente da parte di personale autorizzato dal Ministero, e con il tracciamento degli accessi e di qualsiasi attività eseguita. La Sezione ITS invia e riceve le comunicazioni in modalità sicura, su rete di comunicazione SPC ovvero, tramite Internet, mediante protocollo Transport Layer Security (TLS) per garantire la riservatezza dei dati su reti pubbliche secondo le pertinenti raccomandazioni AgID in materia (Determinazione n. 471 del 5 novembre 2020).