**Articolo 10**

**ALLEGATO 5**
**«Garanzie e misure di sicurezza»**

**1. Introduzione**

Il presente allegato descrive le principali garanzie e misure di sicurezza dell'ANIST, in conformità all'articolo 62-*quater*, comma 6, del CAD.

Per le predette finalità, l'ANIST è dotata di:

- 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;
- un sistema di tracciamento e di conservazione dei dati di accesso alle componenti applicative e di sistema;
- sistemi di sicurezza per la protezione delle informazioni e dei servizi erogati dalla base dati;
- 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;
- una Certification Authority;
- sistemi e servizi di backup per il salvataggio dei dati e delle applicazioni; - sistemi e servizi di Disaster Recovery.

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

**2. 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.

La riservatezza dei dati è, inoltre, garantita attraverso l'adozione di misure di pseudonimizzazione tramite il disaccoppiamento dei dati e il mascheramento delle chiavi di correlazione. I dati ulteriori, necessari ai soli servizi di monitoraggio, sono memorizzati in forma pseudonimizzata in una sezione segregata e distinta della base dati ANIST.

Nel caso di servizi fruiti tramite il Portale ANIST, 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 ANIST sono garantiti attraverso l'apposizione di un sigillo elettronico ad ogni documento.

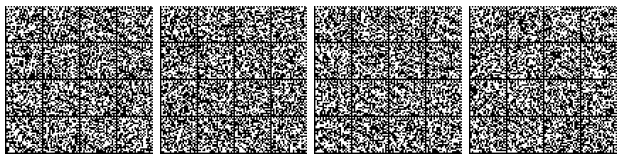
Per la fruizione dei servizi resi fruibili dalla PDND l'integrità e il non ripudio sono garantiti dalle policy proprie della PDND.

**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.).

Il periodo di retention dei dati e dei log sarà definito in apposita policy del Ministero dell'Istruzione e del merito e reso noto ai cittadini nelle informative che saranno rilasciate, rispettando il principio di non eccedenza e, più in generale, la normativa in materia di data protection.

**4. Infrastruttura fisica**

L'infrastruttura di 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.

**5. 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:

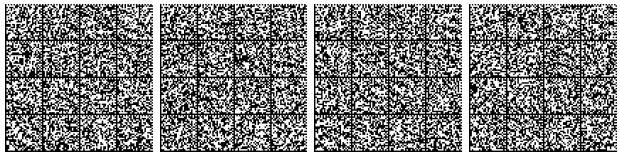
a) aggiornamenti periodici dei sistemi operativi e dei software di sistema e *hardening* delle macchine;
b) adozione di una infrastruttura di sistemi *firewall* e sistemi IPS (*Intrusion Prevention System*), che consentono la rilevazione dell'esecuzione di codice non previsto nonché di azioni in tempo 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*.

**6. Accesso**

L'accesso all'ANIST avviene in condizioni di pieno isolamento operativo e di esclusività, in conformità ai principi di esattezza, disponibilità, accessibilità, integrità e riservatezza dei dati, 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 dell'istruzione e del merito, e con il





tracciamento degli accessi e di qualsiasi attività eseguita. L'ANIST 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).

**Articolo 11, comma 3.**

## ALLEGATO 6

## «Cronoprogramma»

| Attività | Scadenza |
|---|---|
| 1.Analisi | II semestre 2024 |
| 2.Progettazione | II semestre 2025 |
| 3.Sviluppo | I semestre 2026 |
| 4.Attivazione | II semestre 2026 |

---

N O T E

AVVERTENZA:

Il testo delle note qui pubblicato è stato redatto dall'amministrazione competente per materia, ai sensi dell'art.10, comma 3, del testo unico delle disposizioni sulla promulgazione delle leggi, sull'emanazione dei decreti del Presidente della Repubblica e sulle pubblicazioni ufficiali della Repubblica italiana, approvato con D.P.R. 28 dicembre 1985, n.1092, al solo fine di facilitare la lettura delle disposizioni di legge alle quali è operato il rinvio. Restano invariati il valore e l'efficacia degli atti legislativi qui trascritti.

*Note alle premesse*:

— Si riporta l'art. 17 della legge 23 agosto 1988, n. 400 (Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei ministri), pubblicata nella *Gazzetta Ufficiale* 12 settembre 1988, n. 214:

«Art. 17 (*Regolamenti*). — 1. Con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, sentito il parere del Consiglio di Stato che deve pronunziarsi entro novanta giorni dalla richiesta, possono essere emanati regolamenti per disciplinare:

*a)* l'esecuzione delle leggi e dei decreti legislativi nonché dei regolamenti comunitari;

*b)* l'attuazione e l'integrazione delle leggi e dei decreti legislativi recanti norme di principio, esclusi quelli relativi a materie riservate alla competenza regionale;

*c)* le materie in cui manchi la disciplina da parte di leggi o di atti aventi forza di legge, sempre che non si tratti di materie comunque riservate alla legge;

*d)* l'organizzazione ed il funzionamento delle amministrazioni pubbliche secondo le disposizioni dettate dalla legge;

e)

2. Con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, sentito il Consiglio di Stato e previo parere delle Commissioni parlamentari competenti in materia, che si pronunciano entro trenta giorni dalla richiesta, sono emanati i regolamenti per la disciplina delle materie, non coperte da riserva assoluta di legge prevista dalla Costituzione, per le quali le leggi della Repubblica, autorizzando l'esercizio della potestà regolamentare del Governo, determinano le norme generali regolatrici della materia e dispongono l'abrogazione delle norme vigenti, con effetto dall'entrata in vigore delle norme regolamentari.

3. Con decreto ministeriale possono essere adottati regolamenti nelle materie di competenza del ministro o di autorità sottordinate al ministro, quando la legge espressamente conferisca tale potere.

Tali regolamenti, per materie di competenza di più ministri, possono essere adottati con decreti interministeriali, ferma restando la necessità di apposita autorizzazione da parte della legge. I regolamenti ministeriali ed interministeriali non possono dettare norme contrarie a quelle dei regolamenti emanati dal Governo. Essi debbono essere comunicati al Presidente del Consiglio dei ministri prima della loro emanazione.

4. I regolamenti di cui al comma 1 ed i regolamenti ministeriali ed interministeriali, che devono recare la denominazione di "regolamento", sono adottati previo parere del Consiglio di Stato, sottoposti al visto ed alla registrazione della Corte dei conti e pubblicati nella *Gazzetta Ufficiale*.

4-*bis*. L'organizzazione e la disciplina degli uffici dei Ministeri sono determinate, con regolamenti emanati ai sensi del comma 2, su proposta del Ministro competente d'intesa con il Presidente del Consiglio dei ministri e con il Ministro del tesoro, nel rispetto dei principi posti dal decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni, con i contenuti e con l'osservanza dei criteri che seguono:

*a)* riordino degli uffici di diretta collaborazione con i Ministri ed i Sottosegretari di Stato, stabilendo che tali uffici hanno esclusive competenze di supporto dell'organo di direzione politica e di raccordo tra questo e l'amministrazione;

*b)* individuazione degli uffici di livello dirigenziale generale, centrali e periferici, mediante diversificazione tra strutture con funzioni finali e con funzioni strumentali e loro organizzazione per funzioni omogenee e secondo criteri di flessibilità eliminando le duplicazioni funzionali;

*c)* previsione di strumenti di verifica periodica dell'organizzazione e dei risultati;

*d)* indicazione e revisione periodica della consistenza delle piante organiche;