Allegato D

MISURE DI SICUREZZA PER LA PROTEZIONE DEI DATI

INDICE

1. Premessa

Il presente allegato descrive le caratteristiche dell'infrastruttura e le misure adottate per garantire riservatezza, integrità e disponibilità dei dati trattati, nonché la sicurezza dell'accesso ai servizi, il tracciamento delle operazioni effettuate, in conformità all'art. 23 del DPCM 178/2015 (Regolamento in materia di fascicolo sanitario elettronico) e per le finalità dell'art. 2 del presente decreto.

2. Definizioni

Ai fini del presente allegato si intendono per:

a) "Sistema di Identity & Access Management", è un sistema che permette di gestire gli utenti e le connesse autorizzazioni, all'interno di un sistema informativo;

b) "Certification Authority", è un ente di terza parte (trusted third party), pubblico o privato, abilitato a rilasciare un certificato digitale tramite procedura di certificazione che segue standard internazionali e conforme alla normativa europea e nazionale in materia;

c) Certificato client: certificato digitale utilizzato per l'autenticazione ad un sistema informatico;

d) "Profilo di autorizzazione", l'insieme delle informazioni, univocamente associate a una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

e) "Backup", la replicazione delle informazioni al fine di prevenire la definitiva cancellazione o compromissione delle stesse a fronte di eventi accidentali o intenzionali che possano minacciarne l'integrità e la disponibilità;

f) "Disaster recovery", l'insieme delle misure tecniche e organizzative adottate per assicurare, in siti alternativi a quelli primari di produzione, il funzionamento di tutti i servizi, a fronte di eventi che provochino, o possano provocare, l'indisponibilità prolungate.

3. Misure di sicurezza applicate all'INI

Per le finalità di cui al paragrafo 1, l'INI, realizzata presso un'infrastruttura di cui si dirà al paragrafo 3.1, 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;
- una *Certification Authority*;
- sistemi e servizi di *backup* per il salvataggio dei dati e delle applicazioni e di Disaster Recovery.

La base dati dell'INI è sottoposta ad un audit interno di sicurezza con cadenza annuale, al fine di verificare l'adeguatezza delle misure di sicurezza.

3.1 Infrastruttura fisica

L'infrastruttura di INI è realizzata dal Ministero dell'economia e delle finanze attraverso l'utilizzo dell'infrastruttura del Sistema Tessera sanitaria in attuazione di quanto disposto dal comma b dell'art. 382 della legge 11 dicembre 2016, n. 232 (Bilancio di previsione dello Stato per l'anno finanziario 2017 e bilancio pluriennale per il triennio 2017-2019).

I locali sono sottoposti a videosorveglianza continua e sono protetti da qualsiasi intervento di personale esterno, ad esclusione degli accessi di personale preventivamente autorizzato necessari alle attività di manutenzione e gestione tecnica dei sistemi e degli apparati.

L'accesso ai locali avviene secondo una documentata procedura, prestabilita dal Titolare del trattamento, che prevede l'identificazione delle persone che accedono e la registrazione degli orari di ingresso ed uscita di tali persone.

3.2 Registrazione degli utenti ed assegnazione degli strumenti di sicurezza

Gli utenti dell'INI sono le regioni. L'autenticazione delle regioni verso l'INI avviene attraverso certificato client con mutua autenticazione.

L'infrastruttura di Identity e Access Management censisce direttamente le utenze, accogliendo flussi di autenticazione e di autorizzazione, per l'assegnazione dei certificati client di autenticazione.

Il sistema effettua la gestione completa del certificato di autenticazione: assegnazione, riemissione alla scadenza, revoca.

La gestione e la conservazione del *certificato client* è di esclusiva responsabilità del soggetto cui sono state assegnate.

La gestione dei profili di autorizzazione è effettuata dall'Amministratore centrale della sicurezza.

L'Amministratore centrale di sicurezza è nominato tra i dipendenti del Ministero dell'economia e delle finanze.

Viene adottato il seguente modello di identità federata: poiché la regione si configura come un intermediario tra l'INI e l'utente finale, è a carico del sistema regionale la generazione e la firma digitale di un'asserzione, costruita secondo lo standard SAML, che certifica l'utente finale in quanto soggetto identificato dalla regione e che ha facoltà di accedere ai servizi dell'INI. In tal caso le credenziali che utilizza l'utente finale sono gestite dalla regione e non direttamente dall'INI. Il sistema di Identity & Access Management dell'INI verifica la validità della firma digitale contenuta nell'asserzione. A tal fine, la Certification Authority emette i certificati per la firma digitale delle asserzioni. Le asserzioni sono firmate dalla regione con un certificato rilasciato dall'INI. Il certificato è firmato da una CA esterna.

La Certification Authority del MEF emette . i certificati per i server regionali L'installazione dei certificati dei server regionali è a carico dell'Amministratore centrale della sicurezza, la loro gestione è a carico dell'infrastruttura di *Identity e Access Management.* La non esportabilità dei certificati dei server regionali è garantita dalla presenza di un codice PIN, generato in fase di installazione sulla specifica postazione destinataria, la cui conservazione è di esclusiva responsabilità dell'amministratore Centrale della sicurezza.

3.3 Sistema di monitoraggio dei servizi

Il Ministero dell'economia e delle finanze, attraverso l'infrastruttura di cui al paragrafo 3.1, eroga i servizi di cui all'allegato A e assolve le funzionalità di sicurezza descritte nel presente allegato, nel rispetto delle specifiche tecniche approvate dal Ministero dell'economia e delle finanze e dal Ministero della salute.

Per il monitoraggio dei servizi, il Ministero dell'economia e delle finanze si avvale di uno specifico sistema di reportistica.

3.4 Sistema di log analysis

Il Ministero dell'economia e delle finanze adotta un sistema di log analysis per l'analisi periodica delle informazioni registrate nei file di log, in grado di 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, per la verifica della correttezza e legittimità del trattamento dei dati, le seguenti informazioni: il codice identificativo del soggetto che ha effettuato l'accesso, la data e l'ora dell'accesso, l'operazione effettuata, il codice identificativo dell'assistito oggetto di consultazione.

I file di log presentano le seguenti caratteristiche:

a) integrità e inalterabilità

b) sono protetti con idonee misure contro ogni uso improprio

c) sono accessibili solo agli incaricati del trattamento esclusivamente in forma aggregata; sono trattati in forma non aggregata unicamente laddove ciò risulti indispensabile ai fini della verifica correttezza e legittimità delle singole operazioni effettuate

d) sono conservati per un periodo di dodici mesi al termine del quale sono cancellati.

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

3.5 Protezione da attacchi informatici

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

a) apposite procedure di profilazione al fine limitare l'operatività alle sole funzionalità necessarie per i 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) infrastruttura di sistemi *firewall* e sistemi IPS (Intrusion Prevention System) che consentono la rilevazione dell'esecuzione di codice non previsto e l'esecuzione di azioni in tempo reale quali il blocco del traffico proveniente da un indirizzo IP attaccante.

3.6 Sistemi e servizi di backup e recovery dei dati soggetti al trattamento

I sistemi e servizi di backup per il salvataggio dei dati e delle applicazioni e di Disaster Recovery, vengono predisposti in conformità all'articolo 34, comma 1, lettera f), del decreto legislativo 30 giugno 2003, n. 196, e ai punti 18 e 23 dell'allegato disciplinare tecnico (Allegato B al decreto legislativo 30 giugno 2003, n. 196).

Il piano di continuità operativa e il relativo piano di disaster recovery, già presente per il Sistema TS, è aggiornato a fronte dell'istituzione dell'INI.

3.7 Canali di comunicazione

L'INI invia e riceve le comunicazioni in modalità sicura, su rete di comunicazione SPC ovvero tramite Internet, mediante protocollo TLS per garantire la riservatezza dei dati. I protocolli di comunicazione TLS, gli algoritmi e gli altri elementi che determinano la sicurezza del canale di trasmissione protetto sono continuamente adeguati in relazione allo stato dell'arte dell'evoluzione tecnologica.

4. Accesso alla base dati

L'accesso all'INI, sia per le funzioni applicative che per gli amministratori di sistema/DBA, 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.

I sistemi di sicurezza garantiscono che l'infrastruttura di produzione sia logicamente distinta dalle altre infrastrutture del Ministero dell'economia e delle finanze e che l'accesso alla stessa avvenga in modo sicuro, controllato, e costantemente tracciato, esclusivamente da parte di personale autorizzato dal Ministero dell'economia e delle finanze, e con il tracciamento degli accessi e di qualsiasi attività eseguita.

4.1 Accesso da parte degli utenti

L'accesso all'INI da parte delle regioni avviene tramite *web services*.

L'autenticazione avviene tramite certificato client (mutua autenticazione) su canale cifrato TLS. I certificati client sono emessi dalla Certification Authority.

Le operazioni effettuate presso la postazione della regione sono registrate nel sistema di *Identity e Access Management*, che registra le informazioni di autenticazione e gli attributi e li utilizza per verificare i diritti di accesso all'informazione e per alimentare il sistema di tracciamento.

5. Misure di sicurezza applicate all'INI-FSE per il regime di sussidiarietà

In regime di sussidiarietà l'INI adotta le misure di sicurezza previste dall'art. 23 del DPCM 178/2015, ad eccezione delle misure di conservazione che restano a carico delle regioni.