Politica generale di sicurezza informatica dell'Agenzia Provinciale per i Pagamenti

Indice generale

Versione 1.0

1 Introduzione

L'Agenzia Provinciale per i Pagamenti (di seguito anche APPAG o Agenzia) è stata istituita dalla legge provinciale 28 marzo 2003, n. 4 - art. 57. All'APPAG sono attribuite (ai sensi dei regolamenti (CE) n. 1290/2005 e n. 885/2006) le funzioni di organismo pagatore degli aiuti derivanti dalla politica agricola comune per la Provincia autonoma di Trento.

Con regolamento emanato con decreto del Presidente della Provincia n. 16-96/Leg. di data 2 luglio 2007, entrato in vigore il 26 settembre 2007, si è provveduto alla disciplina dell'organizzazione e del funzionamento di APPAG.

Secondo quanto disposto dall'art. 7, comma 2, del regolamento sopra citato, l'Agenzia provinciale per i pagamenti si articola in:

- Direzione e affari generali;
- Controllo interno;
- Sistema informativo;
- Unità tecnica e di autorizzazione;
- Unità di esecuzione pagamenti;
- Unità di contabilizzazione.

Tale struttura organizzativa è stata definita in modo da garantire la separazione delle funzioni di autorizzazione, esecuzione e contabilizzazione dei pagamenti, nonché la costituzione di servizi di controllo interno e tecnico, così come stabilito nei criteri previsti per il riconoscimento dell'organismo pagatore dal regolamento CE n. 885/2006 (successivamente modificato dal regolamento CE n. 1233/2007).

Al punto 3 lettera "B", gli stessi criteri recitano inoltre:

"La sicurezza dei sistemi d'informazione si basa su criteri definiti in una versione applicabile, nell'esercizio finanziario di cui trattasi, di una delle seguenti norme internazionalmente riconosciute:

i) Organizzazione internazionale per la standardizzazione 27002: Code of practice for Information Security management (ISO) (codice di buona pratica per la gestione della sicurezza delle informazioni);

ii) Bundesamt für Sicherheit in der Informationstechnik (Ufficio federale per la sicurezza delle tecniche dell'informazione): IT-Grundschutzhandbuch/IT manuale di sicurezza informatica di base (BSI);

2006R0885—IT —30.10.2007 — 001.001— 18 (1) GU L 205 del 3.8.1985, pag. 5.

iii) Information Systems Audit and Control Foundation: Control Objectives for Information and related Technology (COBIT) (obiettivi di controllo nel campo dell'informazione e delle tecnologie correlate).

L'organismo pagatore sceglie una delle norme internazionali di cui al primo comma quale base della sicurezza dei propri sistemi d'informazione.

Occorre che le misure di sicurezza siano adeguate alla struttura amministrativa, al personale e all'ambiente tecnologico di ciascun organismo pagatore. Lo sforzo finanziario e tecnologico deve inoltre essere proporzionale ai rischi effettivi."

APPAG ha scelto ISO27001:2005 quale norma internazionale di riferimento poiché adottata anche dalla Provincia Autonoma di Trento, di cui l'Agenzia fa parte, e da Informatica Trentina spa, responsabile del Sistema Informativo Elettronico Provinciale di cui fa parte il Sistema Informativo Agricolo Provinciale (SIAP). In fase di avvio l'APPAG si avvale dei servizi del Sistema Informativo Agricolo Nazionale (SIAN) e, per quanto riguarda il Sistema di Gestione della Sicurezza delle Informazioni, fa riferimento a quello adottato dalla società incaricata da AGEA per la sua gestione.

2 Ambito di applicazione

Questa politica generale di sicurezza costituisce un quadro di riferimento che deve essere applicato:

- da APPAG;
- da tutte le strutture della Provincia Autonoma di Trento che sono coinvolte dall'attività dell'Agenzia;
- da Informatica Trentina in quanto responsabile della gestione del Sistema informativo elettronico provinciale;
- da tutti i responsabili esterni dei trattamenti di cui si avvale APPAG.

Questo documento, approvato dalla Direzione di APPAG, è stato predisposto dall'Ufficio del sistema informativo dell'Agenzia d'intesa con Informatica Trentina Spa e Servizio Organizzazione ed Informatica della PAT che ne condividono tutti i contenuti.

Di seguito sono individuati i principali ruoli e le principali responsabilità di carattere decisionale previsti per la gestione della sicurezza delle informazioni che APPAG tratta nell'esercizio delle proprie funzioni istituzionali.

3 Individuazione dei ruoli

3.1 Provincia Autonoma di Trento

APPAG si configura come struttura provinciale e quindi, ai sensi della normativa sulla protezione dei dati personali, designa la Provincia Autonoma di Trento come persona giuridica nel suo complesso, titolare dei trattamenti di dati personali svolti per le sue finalità istituzionali. Nell'esercizio delle funzioni di titolare del trattamento e, di conseguenza, nel perseguimento delle finalità indicate dalla presente politica generale di sicurezza, la Provincia opera in concreto attraverso gli organi ed i soggetti di volta in volta competenti in base alle disposizioni ordinamentali; in particolare la Giunta provinciale ha la competenza di adottare atti generali di carattere organizzativo e procedurale o direttive.

3.2 Dirigente della struttura competente in materia di organizzazione e informatica

Al Dirigente della struttura competente in materia di organizzazione e informatica spettano l'individuazione di specifiche istruzioni operative a garanzia della sicurezza, ad integrazione e chiarimento di quelle stabilite dalla Giunta provinciale e l'assistenza tecnica alle strutture in ordine all'applicazione delle misure di sicurezza per il trattamento dei dati personali.

3.3 Direttore dell'Agenzia Provinciale per i Pagamenti

Spettano al Direttore di APPAG, le funzioni che hanno a che fare con decisioni e scelte attinenti l'attività gestionale e la vigilanza sull'applicazione delle misure di sicurezza da parte del personale assegnato alle strutture di propria competenza.

Qualora il direttore lo ritenga opportuno, al fine di rispettare gli standard derivanti dalla normativa comunitaria e nazionale in materia di organismi pagatori, può adottare ulteriori misure di sicurezza.

3.4 Informatica Trentina SpA - Responsabile della gestione del SIEP

L'amministratore di sistema è il soggetto cui è conferito il compito di sovrintendere alle risorse di un sistema informativo elettronico e di consentirne l'utilizzazione. La Giunta provinciale, con propria deliberazione n. 3217 di data 23 dicembre 2002, ha incaricato di nominare gli amministratori di sistema Informatica Trentina SpA per i sistemi operativi presenti su elaboratori in uso presso le strutture provinciali affidati alla gestione della società medesima. Poiché tutte le risorse assegnate al SIEP, compreso il SIAP, sono gestite da Informatica trentina, spettano alla società e ai soggetti da essa preposti le funzioni di controllo e coordinamento che non sono riservati ai responsabili delle strutture provinciali in quanto responsabili dei trattamenti ai sensi del Dlgs n. 196/2003. Di conseguenza le indicazioni generali del presente documento si applicano anche a Informatica Trentina.

3.5 Utenti

Gli utenti condividono le responsabilità per la protezione delle risorse loro affidate, incluse le informazioni e gli strumenti informatici. Tutto il personale deve essere accuratamente informato sulle politiche di sicurezza adottate e deve prontamente evidenziarne ogni violazione, anche sospetta, al proprio responsabile.

4 Principi di sicurezza

I principi fondamentali su cui APPAG fonda la propria gestione della sicurezza delle informazioni sono contenuti nel Documento Programmatico della Sicurezza che la Provincia Autonoma di trento approva annualmente con propria deliberazione e che si basa su due distinti documenti di analisi dei rischi: il primo relativo a quelli di competenza delle strutture provinciali, il secondo di competenza di Informatica trentina spa. Entrambi, per motivi di riservatezza, non sono allegati al presente documento, ma possono essere visionati su richiesta presso i rispettivi titolari.

Di seguito sono ripresi alcuni di questi pricipi generali; per gli tutti gli altri aspetti si rimanda al Documento Programmatico della Sicurezza sopra citato (allegato A del presente documento).

4.1 Organizzazione della sicurezza all'interno di APPAG

L'implementazione ed il controllo della sicurezza dei beni all'interno di APPAG devono essere regolati e coordinati. In particolare i soggetti coinvolti, secondo quanto definito nella funzione assegnata, devono provvedere a:

- definire, approvare e applicare le politiche di sicurezza e le relative procedure;
- definire le modalità di valutazione del rischio e la scelta delle contromisure per la sua riduzione;
- implementare i controlli di sicurezza;
- monitorare la correttezza e l'efficacia del sistema implementato.

4.2 Inventario e classificazione delle risorse

Le risorse informatiche utilizzate a supporto delle attività, indipendentemente dal tipo, dal formato e dai supporti di memorizzazione o di comunicazione, devono essere gestite al fine di preservare la loro riservatezza e criticità

Da tale principio consegue che deve essere:

- predisposto e mantenuto un inventario dei beni;
- individuato un proprietario per ogni bene;
- classificato ogni bene al fine di permettere l'adozione di misure di sicurezza commisurate al valore del bene stesso.

4.3 Personale

Il personale di APPAG è parte attiva del processo di gestione del rischio di sicurezza e quindi deve essere a conoscenza della politica generale della sicurezza e delle procedure di sicurezza adottate. Ne consegue che il personale deve:

- essere informato circa le proprie responsabilità in tema di sicurezza
- essere adeguatamente formato e sensibilizzato, secondo appositi piani di formazione in funzione dei ruoli e delle responsabilità di sicurezza attribuiti, per il rispetto puntuale dei principi e l'applicazione delle regole adottate operare seguendo scrupolosamente le regole di sicurezza definite, facendosi portatore nei confronti della dirigenza di suggerimenti e richieste
- segnalare ogni incidente o sospetto tale, e ogni comportamento non in linea con quanto definito, secondo le procedure di comunicazione predisposte.

4.4 Sicurezza fisica

I beni devono essere protetti tramite la predisposizione e il mantenimento di un ambiente fisico che impedisca la fuoriuscita di materiali ed il verificarsi di danni. Tale principio deve essere perseguito attraverso misure di controllo, correlate ai rischi e al valore dei beni. Ne fanno parte le seguenti componenti:

- la definizione e la classificazione dei perimetri di sicurezza
- l'implementazione di misure di sicurezza negli ambienti definiti
- il corretto posizionamento delle risorse fisiche all'interno dei perimetri in relazione alla classificazione di sicurezza
- la tempestiva rilevazione di eventi anomali.

4.5 Gestione operativa e delle comunicazioni

L'infrastruttura tecnica deve essere gestita in modo efficace ed efficiente nel tempo al fine di garantire che all'utente sia fornito il livello di servizio richiesto e che i beni (materiali e immateriali) siano gestiti, anche nel trasferimento, in modo da preservarne la riservatezza e la criticità. Pertanto:

- gli aggiornamenti dell'hardware, del software di base e degli applicativi devono essere pianificati e autorizzati al fine di minimizzare gli impatti sul livello di servizio;
- le procedure di autorizzazione e di implementazione devono essere rispondenti ai differenti requisiti di sicurezza e di continuità in relazione alla diversa tipologia di intervento;
- la gestione dei cambiamenti deve essere disciplinata da apposita procedura, inserita e gestita nel sistema di gestione della sicurezza informatica;
- i test di modifiche strutturali o evolutive devono essere effettuati in un ambiente dedicato a tale scopo.

A questo proposito, il processo di collaudo del software deve essere condotto secondo le specifiche di test:

- i dati di produzione non devono essere utilizzati per scopi di test senza che ogni informazione riservata e ogni dato personale sia prima rimosso o modificato in modo da preservare i dati stessi;
- gli incidenti (malicious software, virus, etc.) devono essere gestiti tramite procedure formalizzate;
- il trasferimento e la comunicazione delle risorse informatiche devono essere normate tramite apposite procedure documentate.

4.6 Controllo accessi logici

La sicurezza deve essere un elemento costitutivo nella fase di sviluppo e di progettazione di nuovi prodotti/sistemi/servizi di APPAG e i prodotti/servizi, sviluppati da o per conto della stessa, devono rispettare requisiti di sicurezza definiti sulla base di una specifica analisi dei rischi, pertanto:

- l'accesso alle risorse informatiche deve essere autorizzato formalmente in base alle reali esigenze operative;
- la gestione delle credenziali degli utenti e dei loro profili di accesso alle risorse devono essere definite tramite procedure, supportate da appositi strumenti software e/o hardware;
- gli utenti autorizzati devono essere responsabilizzati all'osservanza delle procedure e delle misure di sicurezza definite.

4.7 Progettazione e sviluppo prodotti/servizi

La disponibilità dei servizi erogati deve essere garantita, in funzione della loro criticità, al fine di assicurare il ripristino dei processi critici entro termini tollerabili, per quanto riguarda l'operatività sia interna sia esterna. Durante le fasi di sviluppo e di progettazione di nuovi prodotti/sistemi/servizi devono essere eseguite le seguenti attività:

per i prodotti/sistemi/servizi che richiedano un elevato livello di sicurezza, deve essere svolta un'adeguata valutazione del rischio di sicurezza che porti alla definizione di controlli atti a diminuire il rischio;

implementazione dei controlli organizzativi, procedurali e tecnologici necessari;

gestione del sistema di sicurezza implementato, che comprenda anche la manutenzione correttiva ed evolutiva.

4.8 Continuità del servizio

Le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della continuità del servizio devono essere formalizzate all'interno di una struttura documentale basata su un piano di continuità che preveda l'individuazione di:

- ruoli e responsabilità coinvolte nel mantenimento della continuità;
- criteri al fine di individuare i processi/servizi critici;
- requisiti di continuità.

Il piano inoltre deve fornire le linee guida in merito alle misure preventive (organizzative e tecnologiche) e alla procedura di escalation, sulla base dei livelli di gravità del danno emergente.

4.9 Conformità

Qualsiasi comportamento deve essere conforme alla normativa di legge inerenti l'ambito dei sistemi informativi e l'ambiente ICT nonché al trattamento di dati personali, alle disposizioni interne e deve essere verificato e garantito nel tempo.

Per conformità si intendono i seguenti adempimenti:

- adozione delle misure richieste per la protezione dei dati personali
- definizione e documentazione dei requisiti normativi e contrattuali
- adozione delle misure richieste per rispettare gli obblighi contrattuali sul copyright
- conformità ai requisiti di legge delle registrazioni da presentare in contenziosi legali
- adozione delle precauzioni necessarie per evitare l'uso illecito delle risorse di elaborazione e comunicazione.