Allegato n. 7

Piano della sicurezza

Il presente "Piano della Sicurezza" riporta, ai sensi dell'art. 4, lettera c, del DPCM 03/12/2013 "Regole tecniche per il protocollo informatico", le misure adottate per la formazione, gestione, trasmissione e interscambio dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali, nel rispetto delle misure minime di sicurezza previste.

Il Sistema di Gestione Informatica dei documenti del Comune di Cessapalombo denominato "PALEO" è accessibile attraverso la rete internet in un server installato presso la T.A.S.K. srl sita in Via Velluti n. 41 a Piediripa di Macerata.

Definizioni

- **misure minime**: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
- **strumenti elettronici**: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- **autenticazione informatica**: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- **credenziali di autenticazione**: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
- **parola chiave**: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- **profilo di autorizzazione**: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- **sistema di autorizzazione**: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Quadro normativo di riferimento

- art. 3 codice privacy – Principio di necessità nel trattamento dei dati
- art. 31 codice privacy – Obblighi di sicurezza
- art. 33 codice privacy – Misure minime
- art. 34 codice privacy – Trattamento con strumenti elettronici
- allegato B codice privacy – Disciplinare tecnico in materia di misure minime di sicurezza

1. Misure di sicurezza e sistema di gestione dei rischi

La sicurezza è *"l'insieme delle misure atte a garantire la disponibilità, l'integrità e la riservatezza delle informazioni gestite"* e dunque l'insieme di tutte le misure atte a difendere il sistema informativo dalle possibili minacce d'attacco.

Sono tre gli aspetti fondamentali relativi alla sicurezza delle informazioni del sistema informativo aziendale:

- **riservatezza:** solo gli utenti autorizzati possono accedere alle informazioni necessarie;
- **integrità:** protezione contro alterazioni o danneggiamenti; tutela dell'accuratezza e completezza dei dati;
- **disponibilità**: le informazioni sono rese disponibili quando occorre e nell'ambito di un contesto pertinente.

L'approccio alla sicurezza avviene in una logica di prevenzione (*risk management*) piuttosto che in una logica di gestione delle emergenze o di semplice controllo/vigilanza.

La costruzione del sistema di sicurezza si articola nelle seguenti fasi principali:

- analisi conoscitiva dell'organizzazione del sistema della sanità elettronica;
- politiche generali di sicurezza delle informazioni;
- analisi e gestione del rischio.

2. Misure di sicurezza dei sistemi e di protezione dei dati

Le azioni necessarie per l'adozione di idonee misure di sicurezza riguardano:

a) la prevenzione: attività che permette di impedire gli accadimenti negativi, agendo direttamente sulla diminuzione delle probabilità di manifestazione dei pericoli;

b) la protezione: attività che permette di diminuire la gravità degli effetti causati eventualmente dall'accadimento dell'evento di pericolo;

c) la garanzia della continuità operativa.

Il processo di gestione dei rischi richiede la necessità di valutare la possibilità di:

- **eliminare il rischio**;
- **ridurre il rischio**;
- **assumere il rischio in proprio**;

- trasferimento a terzi non assicurativo: si pensi alla stipulazione di un contratto con soggetto esterno per il servizio di back-up, che garantisca la ridondanza e la facoltà del ripristino dell'uso e della disponibilità dei dati personali in caso di danneggiamento o di blocco del sistema;
- infine, ma costituisce la soluzione estrema, ove non sia possibile procedere come ai punti precedenti, si può valutare l'ipotesi di stipulare un contratto di assicurazione per il **trasferimento del rischio ad un soggetto terzo dietro pagamento di un premio assicurativo**.

Con specifico riferimento alla protezione dei dati personali, l'articolo 31 del codice della privacy prevede l'obbligo di adottare **misure idonee di sicurezza**, che hanno lo scopo di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Le misure idonee di sicurezza sono adottate secondo la **filosofia dell'autodeterminazione**, per cui si deve provvedere alla riduzione dei rischi, che possono interessare i dati personali oggetto di trattamento in seno alla società e che riguardano il sistema informativo nel suo complesso.

Al fianco delle misure idonee di sicurezza, al fine di favorire un livello omogeneo di sicurezza per ogni soggetto che proceda al trattamento dei dati personali, il legislatore ha previsto (ai sensi dell'articolo 33 del codice della privacy) l'obbligo di adottare **misure minime**, che sono individuate dagli articoli 34 e 35 del codice della privacy e specificate dall'allegato B del medesimo codice.

Le misure minime sono ripartite a seconda della tipologia di strumenti utilizzati ai fini del trattamento (ossia strumenti elettronici e strumenti non elettronici).

3. Analisi del rischio

Sono cinque le tipologie di rischio fondamentali, che possono interessare la gestione dei documenti:

Garanzia	Rischio	Misura di protezione	Check
Riservatezza	Accesso abusivo ai dati	Sistema anti intrusione (firewall)	La Task adotta due sistemi di sicurezza perimetrali, un IPS (Antiintrusione) sulla rete internet ed un sistema di Firewall Iptable nella rete Intranet.
		Sistema di autenticazione	Tutti i sistemi prevedono l'autenticazione con rinnovo delle password trimestrale e con password complesse.
Integrità	Modificazione dei dati	Sistema di autorizzazione	Non tutti gli utenti possono accedere a tutti i dati, ma ognuno di loro accede esclusivamente a quella serie di dati che deve trattare per svolgere le sue

			mansioni. Allo scopo, per ciascun utente, al momento della registrazione nel sistema di protocollo informatico Paleo, viene individuato e configurato un "profilo utente", con il quale effettuare le sole operazioni di trattamento dei dati che le competono. Tali profili di autorizzazioni riproducono la struttura dell'Ente. Una o più volte l'anno, la Task assieme al referente per il protocollo informatico dell'Ente verifica la sussistenza delle condizioni per la conservazione dei profili di autorizzazione di ciascun Ente.
		Antivirus	Tutti i sistemi sono dotati di antivirus aggiornato quotidianamente.
Disponibilità dei dati	Perdita dei dati	Copie di back up con cadenza giornaliera	I server sono sottoposti a backup giornaliero relativamente ai dati contenuti e settimanale relativamente alla macchina virtuale intera.
	Continuità delle registrazioni	Registro di protocollo giornaliero	La predisposizione del registro di protocollo giornaliero, per gli Enti che utilizzano il sistema Paleo, non è completamente automatica, ma è compito del Responsabile del Protocollo, opportunamente addestrato, avviare la procedura di predisposizione del registro. Paleo prevede la procedura di generazione del registro giornaliero, tramite la quale l'utente autorizzato tramite il profilo di "Responsabile del Protocollo" dell'Ente accede alla procedura, chiude il protocollo e genera la stampa di registro per il giorno. A quel punto, Paleo si occupa della generazione del registro e avverte l'utente, tramite mail, dell'esito della procedura. Il registro di protocollo è incluso nell'insieme dei dati sottoposto a backup giornaliero e settimanale.
	Mancanza di alimentazione	Gruppo di continuità	L'intera sala macchine è sotto il Gruppo di continuità che ne garantisce il funzionamento anche in

			assenza di corrente per almeno 4 ore.
		Ridondanza	I gruppi di continuità sono ridondati, in caso di rottura di un Gruppo ne entra in funzione uno esattamente uguale.