SAGI SERVICE SRL
Via Piave 3 - 07100 Sassari
PI-CF: 01677400903

Tel/Fax 079.37.66.077
Email: info@sagiservice.it - www.sagiservice.it

PASSIONE PER IL PUNTO CASSA

REGISTRO DEI TRATTAMENTI

DATI IDENTIFICATIVI DEL REGISTRO	
DQ03/P08 - Rev. 00 del 02.05.2018	
Registro del	21/05/2018
Relativo al periodo:	2017-2018
Verificato e Redatto da:	
Giovanni Battista Scano	Stefano Lai
Direzione	Responsabile Informatico

1. Scopo

Scopo di questo documento è di delineare il quadro delle misure di sicurezza e organizzative, da adottare per il trattamento dei dati personali effettuato da SAGI SERVICE SRL (nel seguito del documento indicato come Titolare).

2. L'elenco dei trattamenti dei dati personali

Al fine di elaborare l'elenco dei trattamenti dei dati, posti in essere dal Titolare, si procede come segue:

- Si individuano i tipi di dati personali trattati, in base alla loro natura
- Si descrivono le aree, i locali e gli strumenti con i quali si effettuano i trattamenti
- Si elabora la mappa dei trattamenti effettuati, che si ottiene incrociando le coordinate dei due punti precedenti.

2.1 Tipologie di dati trattati

I dati trattati dal Titolare si possono suddividere come segue:

a) DATI COMUNI relativi a clienti / fornitori / utenti
b) Dati relativi allo svolgimento di attività economiche ed alle informazioni commerciali
c) DATI COMUNI relativi al personale
d) DATI PARTICOLARI relativi al personale

2.2 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti

Il trattamento dei dati personali avviene presso la sede della Sagi Service sita in Via Piave n. 3 Sassari. Gli uffici sono situati al piano soppalcato dell'immobile citato, di proprietà della Sagi Service srl.

L'accesso a tale ufficio è consentito previo riconoscimento a cura del personale interno del Titolare.

In ogni caso tutti gli avventori dell'ufficio vengono trattenuti in una zona adiacente all'entrata dell'ufficio prima di consentirne l'accesso ai locali. Nel locale di attesa, non sono presenti strumenti e/o attrezzature che potrebbero dare luogo a diffusione involontaria di dati riservati.

Il trattamento dei dati personali avviene con i **seguenti strumenti**:

A – Schedari ed altri supporti cartacei

I supporti cartacei, ivi inclusi quelli contenenti immagini, vengono ordinatamente raccolti in schedari, ovvero nella pratica cui si riferiscono, per essere archiviati, una volta terminato il ciclo lavorativo, come segue:

- Archivio Clienti e Fornitori: in cui si raccolgono le pratiche e gli schedari relativi a clienti e rapporti con i fornitori, di natura normale. Alcuni schedari sono all'interno di un archivio dotato di serratura, altri si trovano all'interno di armadi dotati anch'essi di serratura.
- Archivio Generico: in cui si raccolgono le pratiche e gli schedari relativi ai rapporti con i dipendenti, o ai canditati per diventarlo, tenendo separati i dati particolari. Tutti gli schedari sono all'interno di un archivio dotato di serratura altri si trovano all'interno di armadi dotati di serratura.

B – Elaboratori in rete pubblica

Per elaboratori in rete pubblica si intendono quelli che utilizzano, anche solo per alcuni tratti, reti di telecomunicazione disponibili al pubblico, ivi inclusa la rete Internet.

Si dispone di una rete pubblica costituita da:

N. 6 Postazioni (Personal Computer) dislocate nell'area Uffici ad accesso controllato

N. 1 Server Windows dislocato/i nell'ufficio Assistenza Tecnica, dentro armadio Rack dotato di serratura

N. 2 Stampanti dislocate nell'area Uffici ad accesso controllato

N. 1 Router dislocato nel RACK di proprietà di SAGI SERVICE

Il Firewall è in via di definizione, in quanto si sta valutando la possibilità di acquistare un Software o di usufruire di servizi aggiuntivi forniti dall'operatore telefonico Vodafone.

2.3 La mappa dei trattamenti effettuati

Incrociando le coordinate di cui ai due paragrafi precedenti, si ottiene la mappa dei trattamenti di dati personali effettuati dal Titolare.

In relazione al diverso grado di rischio, è opportuno distinguere i trattamenti che vengono posti in essere nelle due distinte aree in cui sono dislocati gli strumenti, nei casi in cui la circostanza è significativa (per gli schedari e gli elaboratori non in rete).

Il simbolo **0**, apposto nella casella di incrocio, significa che determinati tipi di dati sono trattati con determinati strumenti:

TIPI DI DATI TRATTATI

DATI COMUNI relativi a clienti / utenti /fornitori	**0**		**0**
Dati relativi allo svolgimento di attività economiche e alle informazioni commerciali	**0**		**0**
DATI COMUNI relativi al personale, nonché ai candidati per diventarlo	**0**		**0**
DATI PARTICOLARI relativi al personale	**0**		
	A	**Ac**	**B**

Legenda degli strumenti utilizzati per il trattamento:

A – Schedari ed altri supporti cartacei, nell'ambito dei quali si procede a suddividere:

Ac - quelli custoditi nell'area ad accesso controllato degli uffici;

B – Elaboratori in rete pubblica;

In generale i dati sensibili vengono trattati con l'ausilio di strumenti elettronici adatti a tale scopo, e vengono gestiti unicamente per assolvere obblighi di legge derivanti da obblighi contrattuali che legano Sagi Service Srl ai propri clienti;

2. Mansionario privacy ed interventi formativi degli incaricati

Per il trattamento dei dati personali, il Titolare:

Ha nominato i seguenti responsabili:

- ***RESPONSABILE ESTERNO PER GESTIONE CONTABILE E FISCALE: Chirri Giacomo (vedi lettera incarico e mansionario DQ02/P01)***
- ***RESPONSABILE ESTERNO PER GESTIONE PAGHE: Cattari Antonia Elena (vedi lettera incarico e mansionario DQ02/P01)***
- ***RESPONSABILE ESTERNO PER MEDICO COMPETENTE LAVORO: Nieddu G. Barbara (vedi lettera incarico e mansionario DQ02/P01)***
- ***RESPONSABILE INTERNO PER CUSTODE PASSWORD: Monica Scano (vedi lettera incarico e mansionario DQ02/P01)***
- ***RESPONSABILE INTERNO GESTIONE SISTEMA INFORMATICO: Lai Stefano (vedi lettera incarico e mansionario DQ02/P01)***

Il trattamento dei dati personali viene effettuato solo da **soggetti che hanno ricevuto un formale incarico**, mediante designazione per iscritto di ogni singolo incaricato, con il quale si individua puntualmente l'ambito del trattamento consentito.

Ai soggetti incaricati della gestione e manutenzione del sistema informativo, siano essi interni o esterni all'organizzazione del Titolare, viene prescritto di non effettuare alcun trattamento, sui dati personali contenuti negli strumenti elettronici, fatta unicamente eccezione per i

trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

Le lettere ed i contratti di nomina dei responsabili interni o esterni, le lettere di incarico o di designazione degli incaricati vengono raccolte in modo ordinato, in base all'unità organizzativa cui i soggetti appartengono: in tale modo il Titolare dispone di un quadro chiaro di chi fa che cosa (***mansionario privacy***), nell'ambito del trattamento dei dati personali.
Annualmente, si procede a verificare e, se necessario, aggiornare la definizione dei dati cui gli incaricati sono autorizzati ad accedere e dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.
La stessa operazione viene compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione o manutenzione degli strumenti elettronici.
La valutazione verrà fatta sul modulo DQ03/P08 REGISTRO DEI TRATTAMENTI, mentre qualora sia necessario l'aggiornamento verrà formulata una nuova lettera di incarico.

Sono previsti **interventi formativi degli incaricati del trattamento**, finalizzati a renderli edotti dei seguenti aspetti:

- Profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l'attività svolta dagli incaricati, e delle conseguenti responsabilità che ne derivano;
- Rischi che incombono sui dati;
- Misure disponibili per prevenire eventi dannosi;
- Modalità per aggiornarsi sulle misure di sicurezza, adottate dal titolare.

Tali interventi formativi sono programmati in modo tale, da avere luogo al verificarsi di una delle seguenti circostanze:

- Al momento dell'ingresso in servizio;
- In occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali;
- In occasione dell'introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi possono avvenire sia all'interno, a cura del Titolare o di altri soggetti esperti nella materia, sia all'esterno, presso soggetti specializzati e vengono registrati e gestiti come da procedura P01- ORGANIZZAZIONE AZIENDALE.

3. Analisi dei rischi che incombono sui dati

La stima del rischio complessivo, che grava su un determinato trattamento di dati, è il risultato della combinazione di due tipi di rischi:

- Quelli insiti nella tipologia dei dati trattati, che dipendono dalla loro appetibilità per soggetti estranei all'organizzazione, nonché dalla loro pericolosità per la privacy dei soggetti cui essi si riferiscono;
- Quelli legati alle caratteristiche degli strumenti utilizzati per procedere al trattamento dei dati.

Si stima il grado di rischio, che dipende dalla **tipologia dei dati trattati dal Titolare**, combinando il fattore della loro appetibilità per i terzi, con quello che esprime la loro pericolosità per la privacy del soggetto cui i dati si riferiscono:

GRADO DI INTERESSE PER I TERZI					
	ELVATISSIMO				
	ALTO				
	MEDIO				
	BASSO	**1** DATI COMUNI relativi a clienti / utenti /fornitori **2** Dati relativi allo svolgimento di attività economiche e alle informazioni commerciali **3** DATI COMUNI relativi al personale, nonché ai candidati per diventarlo **4** DATI PARTICOLARI relativi al personale			
		BASSO	**MEDIO**	**ALTO**	**ELEVATISSIMO**

PERICOLOSITA' PER LA PRIVACY DELL'INTERESSATO

- Si nota che il titolare, per via dell'oggettiva attività svolta, tratta dati il cui interesse per i terzi è sostanzialmente basso.

Per quanto concerne gli **strumenti impiegati per il trattamento**, le componenti di rischio possono essere idealmente suddivise in:

1. Rischio di area, che dipende dal luogo dove gli strumenti sono ubicati. Tale rischio è legato sostanzialmente:
   - Al verificarsi di eventi distruttivi (incendi, allagamenti, corto circuiti);
   - Alla possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici);
2. Rischio di guasti tecnici delle apparecchiature, che interessa in particolare gli strumenti elettronici (risorse hardware, software e supporti);
3. Rischio di penetrazione logica nelle reti di comunicazione;
4. Rischio legato ad atti di sabotaggio e ad errori umani, da parte del personale appartenente all'organizzazione del Titolare, o di persone che con essa hanno stretti contatti.

Nella seguente tabella si evidenziano i fattori di rischio cui sono soggetti gli strumenti con cui l'organizzazione procede al trattamento dei dati personali. Il simbolo **O**, posto nella casella di intersezione, significa che l'esposizione al rischio è modesta; il simbolo **X** significa che l'esposizione al rischio è elevata

TIPI DI DATI TRATTATI

Rischio d'area, legato al verificarsi di eventi distruttivi	**O**	**O**
Rischio d'area, legato all'accesso non autorizzato nei locali	**O**	**O**
Rischio di guasti tecnici di hardware, software e supporti	**O**	**O**
Rischio di penetrazione logica nelle reti di comunicazione	**O**	**O**
Rischio legato ad atti di sabotaggio e ad errori umani	**O**	**O**
	A	**B**

Legenda degli strumenti utilizzati per il trattamento:
A – Schedari ed altri supporti cartacei
B – Elaboratori in rete pubblica

Nell'elaborare la tabella, si è tenuto conto anche di alcuni fattori legati alla struttura del Titolare, nei seguenti termini:

- Il rischio d'area, legato all'eventualità che persone non autorizzate possano accedere nei locali in cui si svolge il trattamento è giudicato di bassa rilevanza in quanto tutta l'area è ad accesso controllato, con conseguente diminuzione del rischio:

- Per gli archivi esistenti in tale area;
- Per gli elaboratori in rete pubblica, in relazione al fatto che i server sono ubicati in tale area;

- Il rischio di guasti tecnici delle apparecchiature interessa i soli strumenti elettronici, che tuttavia vengono utilizzati da personale competente;
- Il rischio di penetrazione logica nelle reti di comunicazione interessa, essenzialmente, i soli strumenti che sono tra loro collegati tramite una rete di comunicazione accessibile al pubblico;
- Il rischio legato ad atti di sabotaggio, o ad errori umani delle persone, è presente in tutte le tipologie di strumenti utilizzati.

4. Misure atte a garantire l'integrità e la disponibilità dei dati

Per quanto concerne il rischio d'area, legato ad eventi di carattere distruttivo, si evidenzia quanto segue:

4.1 La protezione di aree e locali

I locali nei quali si svolge il trattamento sono dotati di estintori in caso di incendio fortuito. Per tali estintori la Sagi Service ha stipulato un contratto di noleggio. Gli stessi estintori vengono pertanto controllati e verificati ogni 6 mesi direttamente dal fornitore. All'interno dell'azienda il personale è formato per l'emergenza antincendio, così come da D.lgs 81/08.
L'impianto elettrico è stato installato in ottemperanza delle vigenti leggi.
Per il rischio di allagamento si sottolinea che essendo uno stabile commerciale non esistono, nell'area interessata condotte idriche relative agli usi domestici, salvo i bagni che rimangono comunque separati dall'area interessata al trattamento. I locali nei quali si svolge il trattamento non sono, inoltre, adiacenti a fiumi e/o corsi d'acqua.
Si prevede inoltre di dotare la rete elettrica da cui sono alimentati gli strumenti elettronici utilizzati per il trattamento dei dati, di un gruppo UPS con la funzione di stabilizzatore di tensione.
Per quanto riguarda le misure atte ad impedire gli accessi non autorizzati, gli edifici ed i locali nei quali si svolge il trattamento sono protetti da vigilanza da parte del personale interno, il quale non è autorizzato a far accedere all'Ufficio persone estranee all'attività stessa, salvo autorizzazione esplicita del Titolare.
Gli impianti ed i sistemi di cui è dotata l'organizzazione:

- **Hanno necessità di aggiornamento software, in particolare di essere aggiornati ad una versione del sistema operativo più recente e performante anche a livello di sicurezza;**

- **Hanno necessità di una protezione antivirus (in via di valutazione il pacchetto della Vodafone che comprende l'antivirus, insieme al Firewall)**

4.2 La custodia e l'archiviazione di atti, documenti e supporti

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti diversi si è provveduto ad istruire gli incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.
Agli incaricati vengono date disposizioni, per iscritto, di accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbi, è stato loro prescritto di rivolgersi ad un superiore, o ad un responsabile del trattamento.
Di conseguenza, agli incaricati è prescritto di prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi riporli nell'archivio, al termine di tale ciclo o comunque al termine della giornata lavorativa.
Gli incaricati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative.
Per quanto concerne l'archiviazione, il Titolare ha adibito appositi schedari, nei quali conservare ordinatamente documenti, atti e supporti contenenti dati personali, in modo distinto per le diverse funzioni aziendali. Tali schedari sono dotati di chiavi.

Gli impianti e le attrezzature, di cui è dotato il Titolare per la custodia e l'archiviazione di atti, documenti e supporti:

- Appaiono soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali contenuti in tali atti, documenti e supporti

4.3 Le misure logiche di sicurezza

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si adottano le seguenti misure:

- Realizzazione e gestione di un sistema di autenticazione informatica, che ha il fine di accertare l'identità delle persone, affinché ad ogni strumento elettronico possa accedere solo chi è autorizzato;
- Realizzazione e gestione di un sistema di autorizzazione, che ha il fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono

effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative;

- Realizzazione e gestione di un sistema di protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus);

Per realizzare le credenziali di autenticazione si utilizzano i seguenti metodi:

- Si associa un codice per l'identificazione dell'incaricato (*username)*, attribuito da chi amministra il sistema, ad una parola chiave riservata (*password*), conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente (almeno trimestralmente)

Agli incaricati vengono impartite precise istruzioni in merito ai seguenti punti:

- Dovere di custodire i dispositivi, attribuiti agli incaricati a titolo di possesso ed uso esclusivo, con i quali si può accedere agli strumenti informatici, la custodia deve avvenire in modo diligente, sia nell'ipotesi in cui tali dispositivi siano riposti negli uffici, che in quella in cui l'incaricato provveda a portare il dispositivo con sé. In ipotesi di smarrimento, l'incaricato deve provvedere immediatamente a segnalare la circostanza all'amministratore di sistema, o alle altre persone che sono state a tale fine indicate, al momento dell'attribuzione del dispositivo;
- Obbligo di non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza;
- Dovere di elaborare in modo appropriato la password, e di conservare la segretezza sulla stessa, nonché sulle altre componenti riservate della credenziale di autenticazione (username), attribuite dall'amministratore di sistema. Agli incaricati è imposto l'obbligo di provvedere a modificare la password, con la seguente tempistica:
  - Immediatamente, non appena viene consegnata loro da chi amministra il sistema;
  - Successivamente, almeno ogni tre mesi.

  Le password possono essere composte da lettere (maiuscole o minuscole) e numeri, devono essere composte da almeno otto caratteri e non devono contenere riferimenti agevolmente riconducibili all'incaricato.

  La password è strettamente personale, pertanto non va condivisa né comunicata a nessuna funzione aziendale, fatta eccezione del Custode delle parole chiave.

La modifica della password (da fare ogni tre mesi) va comunicata al Custode delle parole chiave che ne prenderà nota nel Registro password.
Nei casi di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe però rendersi necessario disporre della password dell'incaricato, per accedere agli strumenti ed ai dati. A tale fine il responsabile del sistema informatico può intervenire sul singolo profilo annullando la password, che verrà modificata al primo accesso dell'incaricato.
La password deve essere immediatamente sostituita, dandone comunicazione al Custode delle Parole chiave, nel caso si sospetti che la stessa abbia perso la segretezza.)

Per quanto concerne le **tipologie di dati ai quali gli incaricati possono accedere**, ed i trattamenti che possono effettuare, si osserva che:

- Non appare necessario prevedere profili di autorizzazione distinti, per le diverse persone, in relazione alle limitate dimensioni della struttura del Titolare ed al fatto che non si ravvisano ragioni di tutela della riservatezza tali, da imporre che uno o più incaricati non possano accedere ad alcune tipologie di dati personali oggetto di trattamento. *Sono stati limitati gli accessi del personale tecnico nel sistema gestionale TREND, al solo scopo di prevenire perdite di dati, dovute alla poca conoscenza dello stesso gestionale.*

Per quanto riguarda la **protezione, di strumenti e dati**, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus), vengono adottate le misure sotto descritte.

1) Il primo aspetto riguarda la protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui all'articolo 615-quinquies del codice penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento (comunemente conosciuti come virus). A tale fine**, nel corso del 2018 ci si doterà di idonei strumenti elettronici e programmi (detto ANTIVIRUS), i quali saranno sottoposti ad aggiornamento automatico dipendente dal rilascio degli aggiornamenti della casa madre. Tutti gli incaricati saranno istruiti, in merito all'utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere, per minimizzare il rischio di essere contagiati.**

2) Il secondo aspetto riguarda la protezione degli elaboratori in rete dall'accesso abusivo, di cui all'articolo 615-ter del codice penale, ai sensi del quale compie tale reato chi si

introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo. La protezione da tali accessi avviene mediante l'impiego di idonei strumenti elettronici, comunemente conosciuti come firewall.

In particolare il sistema informatico è protetto a mezzo di:

Firewall: attualmente non installato, ma in via di valutazione di acquisto o utilizzo di quello fornito dall'operatore telefonico Vodafone;

Software antivirus: attualmente non installato, ma in via di acquisto.

Software antivirus posta elettronica alla fonte (attivato sul Web Server di posta);

L'aggiornamento di tali strumenti avviene o avverrà in base ai rilasci della casa produttrice. Il controllo sull'efficienza e l'efficacia di tali strumenti invece è fatta con cadenza mensile dal responsabile della gestione del sistema informatico nominato.

3) Il terzo aspetto riguarda l'utilizzo di appositi programmi, la cui funzione è di prevenire la vulnerabilità degli strumenti elettronici, tramite la verifica di eventuali inconsistenze e inesattezze nella configurazione dei sistemi operativi e dei servizi di rete, e di correggere di conseguenza i difetti insiti negli strumenti stessi. A tale riguardo la nostra organizzazione si è da tempo dotata di tali programmi, per la protezione da malfunzionamenti degli strumenti elettronici, che provvede ad aggiornare con cadenza almeno annuale, che diventa semestrale per gli strumenti con i quali si trattano eventualmente dati sensibili o giudiziari. Di norma l'aggiornamento sui malfunzionamenti dei sistemi operativi e applicativi (Fix sistemi Operativi) avviene semestralmente, salvo casi particolari dovuti a manutenzione. **??????????????**

5. Criteri e modalità di ripristino dei dati

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli o addirittura distruggerli, vengono previsti criteri e modalità tali, da garantire il loro ripristino in termini ragionevoli, e comunque entro una settimana per i dati sensibili e giudiziari.

In particolare è stata predisposta una procedura di back up dei dati che copre anche le configurazioni sia dei profili sia degli applicativi utilizzati.

Nel caso di totale perdita dei dati, una volta ripristinato l'impianto hardware, tutto l'insieme dei dati e delle configurazioni può essere reintegrato nel massimo di 16 ore lavorative.

In caso di danneggiamento totale dell'impianto informatico si prevede di poter ripristinare la piena operatività nel massimo di 40 ore lavorative (una settimana).

Per i dati trattati con strumenti elettronici, sono previste procedure di backup, attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema, su dispositivi opportuni.

Il salvataggio dei dati trattati avviene come segue:

- La frequenza è giornaliera su supporto interno e settimanale su supporto esterno;
- Il salvataggio viene effettuato con tipologia INCREMENTALE, perciò viene utilizzato lo stesso supporto per tutti i back up;
- L'integrità dei supporti del back up viene verificata con cadenza mensile dal responsabile per la manutenzione del sistema informatico;
- I backup vengono effettuati sia su supporti interni che su hard disk esterno
- Le copie su supporto esterno vengono custodite nella cassaforte aziendale.

6. Controllo generale sullo stato della sicurezza

Al titolare è affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

Al fine di verificare l'efficacia delle misure di sicurezza adottate, il Titolare e le persone da questo appositamente incaricate provvedono con frequenza mensile, anche con controlli a campione, ad effettuare una o più delle seguenti attività:

- Verificare l'accesso fisico ai locali dove si svolge il trattamento;
- Verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- Monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici, mediante l'analisi dei log file, nei quali i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono le operazioni svolte dagli incaricati per il loro tramite. Attraverso questa analisi, che viene effettuata adottando strumenti automatici di reportistica e di sintesi, è possibile individuare i tentativi, riusciti o meno, di accesso al sistema e l'esecuzione di operazioni non corrette, o sospette;
- Verificare l'integrità dei dati e delle loro copie di back-up;
- Verificare la sicurezza delle trasmissioni in rete;
- Verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti definitivamente;
- Verificare il livello di formazione degli incaricati.

Almeno ogni sei mesi, si procede ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da

parte degli incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati in sei mesi.