Allegato “A”

DOCUMENTO PROGRAMMATICO
SULLA SICUREZZA

Aggiornato con Deliberazione n. 65 del 07 aprile 2014

INDICE

Premessa 3

1. Elenco dei trattamenti dei dati personali 3

1.1 Tipologie di dati trattati e categorie di soggetti cui si riferiscono 3

1.2 Locali in cui si effettuano i trattamenti 4

1.3 Strumenti per il trattamento dei dati personali 5

1.3.1 – Schedari ed altri supporti cartacei 5

1.3.2 – Server e SAN (storage area network) 6

1.3.3 – Personal computer 6

2. Distribuzione dei compiti e delle responsabilità 6

2.1. Titolare del trattamento dei dati personali 6

2.1.1 – Compiti del Titolare del trattamento dei dati personali 6

2.2. Responsabili del trattamento dei dati personali 7

2.2.1 – Compiti e nomina dei Responsabili del trattamento dei dati personali 7

2.3. Incaricati del trattamento dei dati personali 8

2.3.1 – Compiti e nomina degli Incaricati del trattamento dei dati personali 8

2.4. Responsabile della gestione e della manutenzione degli strumenti elettronici 9

2.4.1 – Compiti e nomina del Responsabile della gestione e della manutenzione degli strumenti elettronici 9

2.5. Interventi formativi 10

3. Analisi dei rischi che incombono sui dati 10

4. Misure atte a garantire l'integrità e la disponibilità dei dati - prescrizioni 14

4.1 La protezione di aree e locali 14

4.2 La custodia e l'archiviazione di atti, documenti e supporti 15

4.3 Le misure logiche di sicurezza 16

5. Criteri e modalità di ripristino dei dati 18

6. Controllo generale sullo stato della sicurezza 18

Premessa

Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logistiche, da adottare per il trattamento dei dati personali, sensibili e giudiziari effettuato dalla Provincia di Savona.
Nel presente documento si forniscono idonee informazioni riguardanti:

1. l'elenco dei trattamenti di dati personali, mediante:
   - la individuazione dei tipi di dati personali trattati,
   - la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti,
   - la elaborazione della mappa dei trattamenti effettuati, che si ottiene incrociando le coordinate dei due punti precedenti,
2. la distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati e previsione di interventi formativi degli incaricati del trattamento;
3. l'analisi dei rischi che incombono sui dati;
4. le misure, già adottate e da adottare, per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
5. i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento;
6. le procedure da seguire per il controllo sullo stato della sicurezza;
7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati affidati, in conformità al Codice della Privacy (Decreto Legislativo n.196/03) all'esterno della struttura del titolare;
8. l'individuazione, per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

1. Elenco dei trattamenti dei dati personali

Al fine di elaborare l'elenco dei trattamenti dei dati gestiti dal Titolare si è proceduto, mediante elaborazione di apposite schede analitiche aggiornate periodicamente e conservate nella banca dati fruibile nel sito Intranet della Provincia, alla suddivisione dei dati personali trattati per tipologie, a seconda della loro natura (comuni, sensibili e giudiziari) e della categoria di soggetti cui essi si riferiscono (es. fornitori, personale), nonché alla descrizione delle aree, delle banche dati, dei locali e degli strumenti con i quali si effettuano i trattamenti.

1.1 Tipologie di dati trattati e categorie di soggetti cui si riferiscono

La Provincia di Savona tratta i dati personali che appartengono a soggetti interessati in quanto autori, destinatari o partecipi di atti, contratti, elaborati, missive e documenti analoghi prodotti o meno dall'Ente o indirizzati o comunque detenuti nell'ambito dello svolgimento delle sue attività istituzionali.
Il trattamento dei dati personali consiste nelle operazioni o complessi di operazioni di cui all'art. 4, lett. a) del

Decreto Legislativo n.196/2003, nell'ambito delle attività istituzionali svolte dalla Provincia di Savona.
Il trattamento dei dati sensibili e giudiziari è effettuato soltanto ove consentito da norme di legge o di regolamento che identifichino le finalità di interesse pubblico, i tipi di dati e le operazioni su di essi eseguibili.

1.2 Locali in cui si effettuano i trattamenti

Il trattamento dei dati personali viene effettuato nei settori e presso gli uffici situati nei luoghi indicati nella tabella che segue.

Elenco delle sedi

Struttura di riferimento	**Indirizzo**
Direzione Generale	Via Sormano, 12 - Savona
Settore Affari Generali e del Personale	Via Sormano, 12 – Savona Archivio deposito – Via Venezia, 42 r. -SV Via Sormano, 12 - Savona
Settore Servizi Finanziari, Patrimonio e Servizi Informativi	Via Sormano, 12 – Savona
Settore Pianificazione e Programmazione Territoriale	Via Sormano, 12 – Savona Via Amendola, 10 - Savona
Settore Gestione Viabilità, Edilizia e Ambiente	Via Sormano, 12 – Savona Via Amendola, 10 - Savona
Settore Politiche Economiche e del Lavoro *Centro per l'impiego di Savona* *Centro per l'impiego di Albenga* *Centro per l'impiego di Carcare*	Via Molinero – Savona Via Molinero - Savona Regione Bagnoli, 39 – Albenga Via Cornareto, 2 – Carcare
Magazzino spedizioni PC posta Turistica	Via Neghelli 16 – Alassio
Ufficio I.A.T. di Bergeggi	Via Aurelia – Bergeggi
Ufficio I.A.T. di Spotorno	Via Aurelia, 121 – Spotorno
Ufficio I.A.T. di Noli	C.so Italia, 8 – Noli
Ufficio I.A.T. di Varigotti	Via Aurelia, 79 – Varigotti
Ufficio I.A.T. di Finale Ligure	Via S. Pietro, 14 – Finale L.

Struttura di riferimento	Indirizzo
Ufficio I.A.T. Di Final Borgo	P.za Porta Testa – Final Borgo
Ufficio I.A.T. di Bardineto	Via A. Roascio, 5 – Bardineto
Ufficio I.A.T. di Calizzano	P.za S. Rocco - Calizzano
Ufficio I.A.T. di Millesimo	P.za Italia, 2 (c/o Pal.Comunale)- Millesimo
Ufficio I.A.T. di Varazze	C.so Matteotti, 56 – Varazze
Ufficio I.A.T. di Celle Ligure	Via Boagno (c/o Pal. Comunale) – Celle L.
Ufficio I.A.T. di Albissola Marina	P.za Lam, 2 – Albissola M.
Ufficio I.A.T. di Albisola Superiore	Piazza Marinetti, 1 – Albisola Superiore
Ufficio I.A.T. di Savona	Via Paleocapa, 76 r – Savona
Ufficio I.A.T. di Sassello	Via G. B. Badano, 45 – Sassello
Ufficio I.A.T. di Ceriale	Piazza Eroi della Resistenza, s.n. – Ceriale
Ufficio I.A.T. di Albenga	P.za del Popolo,11 – Albenga
Ufficio I.A.T. di Alassio	Via Mazzini, 68 – Alassio
Ufficio I.A.T. di Laigueglia	Piazza Preve, 17 – Laigueglia
Ufficio I.A.T. di Andora	L.go Milano c/o Palazzo Tagliaferro - Andora
Ufficio I.A.T. di Garlenda	Via Roma, 6 – Garlenda
Ufficio I.A.T. di Ortovero	Via Roma, 79 - Ortovero
Ufficio I.A.T. di Borgio Verezzi	Via Matteotti, 173 – Borgio Verezzi
Ufficio I.A.T. di Pietra Ligure	P.za Martiri della Libertà, 30 – Pietra L.
Ufficio I.A.T. di Loano	C.so Europa, 19 Loano
Ufficio I.A.T. di Borghetto S. Spirito	P.za Libertà, 1 – Borghetto S. Spirito
Ufficio I.A.T. di Toirano	Piazzale Grotte - Toirano

1.3 Strumenti per il trattamento dei dati personali

1.3.1 – Schedari ed altri supporti cartacei

I supporti cartacei, compresi 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:

- gli archivi contenenti dati relativi allo stato di salute e dati sensibili in generale e giudiziari sono localizzati in tutte le aree in cui si raccolgono le pratiche e gli schedari, e sono conservati in armadi o cassetti chiusi a chiave e separatamente dagli altri dati trattati in modo tale che vengano consultati e utilizzati solo nei casi strettamente necessari;
- gli archivi contenenti dati personali in generale sono collocati presso tutti gli uffici. Sono adottate idonee

cautele atte a garantire la riservatezza degli interessati, quali custodia dei documenti all'interno di fascicoli privi di indicazioni anagrafiche, anche se i fascicoli non necessariamente sono chiusi in contenitori muniti di chiave;

- l'accesso all'archivio di deposito è controllato e vengono identificati e registrati i soggetti che vi vengono ammessi, con annotazione della documentazione consultata, se utenti esterni, e annotazione della documentazione ritirata dagli utenti interni, corredata dalla data di prelievo e di riconsegna.

1.3.2 – Server e SAN (storage area network)

Per server e SAN si intendono i dispositivi dedicati al trattamento e all'archiviazione dei dati elettronici di qualsiasi natura. Tali dispositivi sono collegati fra loro tramite rete locale e geografica protetta da apparati anti intrusione meglio descritti nel seguito.

1.3.3 – Personal computer

Quasi tutti i dipendenti sono dotati di un personal computer collegato alla rete provinciale, alcuni dipendenti condividono un unico personal computer. Tutti i dipendenti accedono mediante login e password personali.

2. Distribuzione dei compiti e delle responsabilità

In questa sezione è presentata una mappa dei ruoli, dei compiti e la nomina delle figure previste per il trattamento dei dati personali:

- Titolare del trattamento dei dati personali e relativi compiti;
- Responsabile del trattamento dei dati personali, relativi compiti e nomina degli stessi;
- Incaricati del trattamento dei dati personali, relativi compiti e nomina degli stessi;
- Responsabile della gestione e della manutenzione degli strumenti elettronici;
- Pianificazione degli interventi formativi.

2.1 - Titolare del trattamento dei dati personali

2.1.1 –Compiti del Titolare del trattamento dei dati personali

Il Titolare del trattamento dei dati è la Provincia di Savona nella persona del Presidente, in qualità di legale rappresentante, al quale competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Il Titolare del trattamento deve assicurare e garantire direttamente che vengano adottate le idonee misure di sicurezza ai sensi del "Codice in materia di protezione dei dati personali" e del "Disciplinare tecnico in materia di misure minime di sicurezza" tese a ridurre al minimo il rischio di distruzione dei dati, di accesso non autorizzato o di trattamento non consentito, previe idonee istruzioni fornite per iscritto. Il Titolare, inoltre,

individua, nomina ed incarica uno o più Responsabili della sicurezza e del trattamento dei dati.

2.2 –Responsabili del trattamento dei dati personali

2.2.1 –Compiti e nomina dei Responsabili del trattamento dei dati personali

Responsabili del trattamento dei dati personali sono i Dirigenti di Settore nominati dal Titolare, nel prosieguo detti anche solo Responsabili.
Ad essi sono affidate le seguenti responsabilità e compiti:

- garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate;
- redigere ed aggiornare ad ogni variazione l'elenco delle sedi in cui vengono trattati i dati;
- redigere ed aggiornare ad ogni variazione l'elenco delle banche dati oggetto di trattamento;
- definire e successivamente verificare con cadenza semestrale le modalità di accesso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità come specificato in seguito;
- decidere se affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare;
- controllare e garantire, qualora il trattamento dei dati sia stato affidato in tutto o in parte all'esterno della struttura del titolare che tutte le misure di sicurezza riguardanti i dati personali siano applicate;
- individuare, nominare e incaricare per iscritto, qualora il trattamento sia effettuato con mezzi informatici,
  - il Responsabile della gestione e della manutenzione degli strumenti elettronici;
  - gli Incaricati della custodia delle copie delle credenziali;
  - gli Incaricati delle copie di sicurezza delle banche dati;
- custodire e conservare i supporti utilizzati per le copie dei dati;
- individuare, nominare e incaricare per iscritto gli Incaricati del trattamento dei dati personali per le banche dati che gli sono state affidate;
- sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal Codice in materia di protezione dei dati personali;
- dare le istruzioni adeguate agli Incaricati del trattamento effettuato con strumenti elettronici e non elettronici;
- verificare periodicamente, e comunque almeno annualmente, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli Incaricati del trattamento dei dati personali.

Il conferimento degli incarichi dirigenziali, in quanto effettuato dal Titolare del trattamento dei dati personali, comporta anche la designazione dei singoli dirigenti quali “Responsabili” dei dati trattati dal Settore di rispettiva competenza.
La designazione comporta l’assegnazione ai dirigenti dei compiti e delle responsabilità di cui al presente

paragrafo ed ha efficacia per l'intera durata dell'incarico dirigenziale.

Qualora il trattamento dei dati sia affidato in tutto o in parte all'esterno della struttura del Titolare, il Responsabile del trattamento dei dati deve redigere ed aggiornare ad ogni variazione l'elenco dei soggetti che effettuano il trattamento dei dati ed indicare per ognuno di essi il tipo di trattamento effettuato specificando:

- i soggetti interessati;
- il luoghi dove fisicamente avviene il trattamento dei dati stessi;
- i Responsabili del trattamento di dati personali.

Nel caso di affidamento del trattamento dei dati in tutto o in parte all'esterno, è nominato Responsabile del trattamento il legale rappresentante del soggetto al quale è affidato il trattamento medesimo o altra persona dallo stesso designato. In caso non si proceda in tal senso, titolare del trattamento dei dati è il soggetto a cui è affidato il trattamento. Quest'ultima ipotesi, potendosi configurare come comunicazione a soggetti terzi, deve essere espressamente prevista da una specifica disposizione di legge o di regolamento.

Il Responsabile, a cui è stato affidato il trattamento dei dati all'esterno, deve rilasciare una dichiarazione scritta da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento ai sensi della normativa vigente.

Per ogni trattamento affidato ad un soggetto esterno alla struttura del titolare, il Responsabile del trattamento dei dati personali deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.

2.3 - Incaricati del trattamento dei dati personali

2.3.1 –Compiti e nomina degli Incaricati del trattamento dei dati personali

Gli Incaricati del trattamento dei dati, nel prosieguo detti anche solo Incaricati, sono le persone fisiche autorizzate dai Responsabili a compiere operazioni di trattamento sui dati personali.

In particolare gli Incaricati devono osservare le seguenti disposizioni:

- gli Incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali devono conservare con la massima segretezza le parole chiave in loro possesso ed uso esclusivo;
- la parola chiave non deve contenere riferimenti agevolmente riconducibili all'Incaricato;
- gli Incaricati non devono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- gli Incaricati debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- gli atti e i documenti contenenti dati personali sensibili o giudiziari, affidati agli Incaricati per lo

svolgimento dei relativi compiti, devono essere controllati e custoditi dagli Incaricati stessi fino alla restituzione in moda da impedirne l'accesso da parte di persone prive di autorizzazione.

La nomina di ciascun Incaricato deve essere effettuata dai Responsabili mediante provvedimento dirigenziale di incarico notificato agli stessi.

Gli Incaricati devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

Agli Incaricati deve essere assegnata una parola chiave e un codice di autenticazione informatica.

La nomina dell'Incaricato è a tempo indeterminato, e decade per cessazione del rapporto di lavoro, o per assegnazione dell'Incaricato ad altro settore dell'Ente.

La nomina, inoltre, può essere revocata in qualsiasi momento dal Responsabile senza preavviso, ed eventualmente affidata ad altro soggetto.

2.4 Responsabile della gestione e della manutenzione degli strumenti elettronici

2.4.1 Compiti e nomina del Responsabile della gestione e della manutenzione degli strumenti elettronici

Il Dirigente del Settore Servizi Finanziari e Sistemi Informativi, quale responsabile del Servizio Informativo dell'Ente, individua, nomina e incarica per iscritto un Responsabile della gestione e della manutenzione degli strumenti elettronici.

In particolare il Responsabile della gestione e della manutenzione degli strumenti elettronici deve osservare le seguenti disposizioni:

- attivare le credenziali di autenticazione agli Incaricati per tutti i trattamenti effettuati con strumenti informatici;
- definire quali politiche adottare per la protezione dei sistemi contro i virus informatici e verificarne l'efficacia con cadenza almeno semestrale;
- proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers");
- informare i Responsabili della sicurezza dei dati personali nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali;
- sovrintendere al buon funzionamento delle risorse del sistema informatico e delle banche dati.

La nomina del Responsabile della gestione e della manutenzione degli strumenti elettronici é effettuata con la notifica del provvedimento dirigenziale di incarico.

Il Responsabile della gestione e della manutenzione degli strumenti elettronici è a tempo indeterminato e decade per revoca o dimissioni dello stesso e può essere revocata in qualsiasi momento dal Responsabile della sicurezza dei dati personali senza preavviso, ed essere affidata ad altro soggetto.

Soggetti responsabili dei trattamenti di dati personali

Struttura di riferimento	Responsabile
Direzione Generale	Direttore Generale
Settore Affari Generali e del Personale	Dirigente
Settore Servizi Finanziari Patrimonio e Servizi Informativi	Dirigente
Settore Politiche Economiche e del Lavoro	Dirigente
Settore Pianificazione e Programmazione Territoriale	Dirigente
Settore Gestione Viabilità Edilizia ed Ambiente	Dirigente

2.5. Interventi formativi

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:

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

Gli interventi formativi avvengono a cura delle strutture interne preposte che si possono avvalere o di personale interno o di altri soggetti esterni esperti della materia.

3. Analisi dei rischi che incombono sui dati

E' necessario individuare i principali eventi potenzialmente dannosi per la sicurezza dei dati, valutarne le possibili conseguenze e la gravità e porli in correlazione con le misure previste.

Si individua nella tabella denominata "Tabella di rischio", l'elenco degli eventi che possono generare danni e che comportano quindi rischi per la sicurezza dei dati personali. L'elenco identifica pertanto diversi eventi rilevanti per l'analisi dei rischi per la sicurezza dei dati personali.

In relazione a ciascun evento viene individuata una contromisura da adottare in relazione alla valutazione della gravità dell'evento stesso e alla probabilità stimata che esso si verifichi.

TABELLA DI RISCHIO					
Evento		**Gravità stimata**	**Probabilità stimata**	**Coeff. di rischio**	**Misure d'azione per sventare il rischio e per garantire l'integrità e la disponibilità dei dati**
Comportamenti degli operatori	carenza di consapevolezza, disattenzione o incuria	8	8	64	Formazione specifica sulle conseguenze di atteggiamenti sbagliati rispetto alle norme di tutela dei dati personali contenute nel codice e rispetto alla corretta custodia dei dati trattati e delle credenziali di autenticazione assegnate
	comportamenti sleali o fraudolenti	8	1	8	
	errore materiale	8	6	48	Verifica e controllo da parte dei Responsabili dei trattamenti sui comportamenti degli incaricati interni ed esterni
Eventi relativi agli strumenti	azione di *virus* informatici o di codici malefici	8	8	64	Aggiornamento giornaliero dell'antivirus
	spamming o altre tecniche di sabotaggio	8	10	80	Corretta gestione dei firewall e adeguato sistema di autenticazione e autorizzazione all'accesso da parte degli incaricati e dei Responsabili del trattamento ai dati presenti nella rete interna.
	malfunzionamento, indisponibilità o degrado degli strumenti	6	8	48	Adeguato sistema antispamm su server dedicati di posta elettronica.
	accessi esterni non autorizzati	5	2	10	Periodica verifica dello stato di obsolescenza delle attrezzature informatiche assegnate agli incaricati e intercettazione di informazioni in rete conseguente rinnovo o implementazione delle stesse.
	intercettazione di informazioni in rete	5	2	10	Aggiornato sistema di mirroring.
					Esecuzione di opportuni back-up periodici (giornalieri, settimanali e annuali) dei server
					Esecuzione, a cura dell'Incaricato, di opportuni back-up periodici sulle postazioni stand alone in caso contengano dati personali.

TABELLA DI RISCHIO					
Evento		**Gravità stimata**	**Probabilità stimata**	**Coeff. di rischio**	**Misure d'azione per sventare il rischio e per garantire l'integrità e la disponibilità dei dati**
Comportamenti degli operatori	carenza di consapevolezza, disattenzione o incuria	8	8	64	Formazione specifica sulle conseguenze di atteggiamenti sbagliati rispetto alle norme di tutela dei dati personali contenute nel codice e rispetto alla corretta custodia dei dati trattati e delle credenziali di autenticazione assegnate Verifica e controllo da parte dei Responsabili dei trattamenti sui comportamenti degli incaricati interni ed esterni
	comportamenti sleali o fraudolenti	8	1	8	
	errore materiale	8	6	48	
Eventi relativi al contesto	accessi non autorizzati a locali/reparti ad accesso ristretto	10	5	50	Formazione specifica sui comportamenti di tutela dei dati quali: ▪ chiusura a chiave degli armadi contenenti dati personali; ▪ chiusura dei cassetti.
	asportazione e furto di strumenti contenenti dati	8	2	16	
	eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	8	1	8	Installazione di opportuna cassaforte a norma per la custodia dei nastri di back-up. Verifica del corretto funzionamento dei gruppi di continuità a supporto dei server
	guasto ai sistemi complementari (impianto elettrico, climatizzazione..)	2	5	10	Attivazione del climatizzatore nelle stagioni calde.
	errori umani nella gestione della sicurezza fisica	3	3	9	

- La gravità dell'evento viene stimata in ordine di gravità crescente da 1 a 10 punti.
- La probabilità che l'evento si verifichi viene stimata in ordine di probabilità crescente da 1 a 10 punti.
- Il coefficiente di rischio di ciascun evento si ottiene moltiplicando fra loro i due indici di gravità e probabilità. La scala del coefficiente di rischio va da 1 a 100.

Il grado di rischio più alto, o addirittura elevatissimo, è collegato al trattamento dei dati, sensibili e giudiziari, alla tutela dei quali devono quindi essere dedicate particolari attenzioni.

Un particolare riguardo dovranno avere altresì i dati attinenti a comportamenti illeciti o fraudolenti o a procedimenti sanzionatori, disciplinari, amministrativi o contabili a carico dei soggetti interessati che potrebbero essere oggetto di banche dati dell'Ente.

Le componenti di rischio possono essere idealmente suddivise in:

1. 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:
2. rischio di guasti tecnici delle apparecchiature, che interessa in particolare gli strumenti elettronici (risorse hardware, software e supporti) e rischio di penetrazione logica nelle reti di comunicazione;
3. rischio di area, che dipende dal luogo dove gli strumenti sono ubicati. Tale rischio è legato sostanzialmente:
    - al verificarsi di eventi distruttivi o alla perdita di dati (incendi, allagamenti, corti circuiti, smarrimento documenti)
    - alla possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici).

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

Tutti i posti di lavoro della Provincia di Savona sono collegati in rete locale e/o geografica e l'accesso agli stessi è consentito previa autorizzazione; il soggetto utilizzatore si assume contestualmente la responsabilità civile e penale sull'utilizzo di hardware, software e dati.

In relazione al proprio sistema informatico, l'Ente si dota delle misure minime di sicurezza, così come prescritto all'art. 33, nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31 del decreto legislativo n. 196/2003.

Nel presente paragrafo vengono descritte nel dettaglio e ad integrazione delle misure d'azione idonee descritte nella precedente tabella (paragrafo 3.) le misure atte a garantire:

- la protezione delle aree e dei locali (Misure Minime Fisiche), nei quali si svolge il trattamento dei dati personali,
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali, sensibili e giudiziari,
- la sicurezza logica, nell'ambito dell'utilizzo degli strumenti elettronici.

Si procede ora alla descrizione delle misure che risultano già adottate dal Titolare, nel momento in cui viene redatto il presente documento.

4.1 La protezione di aree e locali

Per quanto concerne il rischio d'area, legato ad eventi di carattere distruttivo, gli edifici ed i locali nei quali si svolge il trattamento sono protetti dalle misure contenute nella seguente tabella:

Descrizione misura	Note ed indicazioni per la corretta applicazione
Custodia degli archivi cartacei in armadi chiusi a chiave	Tutti i documenti cartacei contenenti dati personali di tipo sensibile e giudiziario sono conservati in armadi dotati di serratura e, per quelli attinenti allo stato di salute o alla vita sessuale dei soggetti interessati,in maniera separata dai dati personali trattati per finalità che non ne richiede il loro utilizzo. Sarà compito dell'Incaricato che preleva i documenti garantire che i documenti siano riposti, sotto chiave al termine delle operazioni di trattamento.
Continuità dell'alimentazione elettrica	I server sono collegatati ad un gruppo di continuità che garantisce una stabilizzazione dell'energia elettrica erogata. Tale gruppo, in conseguenza di un'improvvisa assenza di energia, garantisce un'autonomia temporale necessaria ad avviare le corrette procedure di spegnimento dell'elaboratore.
Dispositivi antincendio	In prossimità degli uffici sono collocati estintori regolarmente revisionati.
Controllo dell'operatore esterno addetto alla manutenzione	Gli addetti alla manutenzione sono sempre accompagnati dal personale dipendente della Provincia di Savona con la finalità di controllarne l'operato.
Impianto di raffreddamento dei server principali	Tutti i locali tecnici sono climatizzati
Cassaforte	La Provincia di Savona. dispone di una cassaforte idonea a trattenere le copie di Back-Up.
Portineria	L'Ente Pubblico effettua servizio di portineria in quasi tutti gli edifici. Solo in particolari casi l'accesso avviene previo controllo dei dipendenti. Nel caso di archivi contenenti dati sensibili o giudiziari, possono accedervi soltanto persone autorizzate ed i dipendenti, dopo l'orario di chiusura al pubblico, provvedono ad identificare chi accede.

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 (ad esempio CD, dischetti, fotografie, pellicole ecc.), si è provveduto ad istruire gli incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti. L'Ente sta inoltre adottando un sistema di conservazione dei dati sensibili e giudiziari conservati su supporti cartacei che consenta l'archiviazione di questi in maniera separata dagli altri dati personali attinenti al medesimo procedimento che vengono trattati per finalità che non prevedono l'utilizzo dei primi.

4.3 Le misure logiche di sicurezza

Per i trattamenti effettuati con strumenti elettronici, 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, vetustà delle attrezzature e programmi che contengono codici maliziosi (virus), mediante, efficienti antivirus, appositi sistemi antispamming, aggiornati sistemi di mirroring, firewall e adeguate procedure di backup;
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili nei quali sono contenuti dati personali;
- per quanto riguarda i supporti rimovibili contenenti dati giudiziari o sensibili, prescrizione di istruzioni organizzative e tecniche al fine di evitare accessi non autorizzati o trattamenti non consentiti.

Il sistema di autenticazione informatica viene adottato per disciplinare gli accessi a tutti gli strumenti elettronici presenti nell'organizzazione del Titolare.

E' impostata e gestita una procedura di autenticazione che permette di verificare l'identità della persona e quindi di accertare che la stessa sia in possesso delle credenziali di autenticazione per accedere ad un determinato strumento elettronico.

Per realizzare le credenziali di autenticazione si utilizza il seguente metodo: si associa un codice per l'identificazione dell'Incaricato (*username)*, ad una parola chiave riservata (*password*) conosciuta solamente dall'Incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla trimestralmente/semestralmente.

Per l'attribuzione e la gestione delle credenziali per l'autenticazione si utilizzano i seguenti criteri:

- ad ogni Incaricato esse vengono assegnate e associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale.

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 (ad esempio smart card): la custodia deve avvenire in modo diligente, sia nell'ipotesi in cui tali dispositivi siano riposti negli uffici (viene prescritto l'obbligo di utilizzare cassetti con serratura), che in quella in cui l'Incaricato provveda a portare il dispositivo con sé (viene prescritto l'obbligo di custodirlo come se fosse una carta di credito). 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. 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 trimestralmente/semestralmente.

Le password sono composte da almeno otto caratteri numerici e alfanumerici; le password, per maggiore sicurezza, non devono contenere riferimenti agevolmente riconducibili all'interessato, quali date di nascita o nomi dei figli.

Per quanto concerne le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, si osserva che si è impostato un sistema di autorizzazione, al 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. L'unica eccezione si ha nei casi in cui il trattamento riguardi solo dati personali destinati alla diffusione: in questo caso non è necessario predisporre alcun sistema di autorizzazione, poiché i dati trattati sono, per definizione, conoscibili da chiunque.

Le autorizzazioni all'accesso vengono rilasciate e revocate dal responsabile della sicurezza dei sistemi, ovvero da soggetti da questi appositamente incaricati.

Periodicamente, e comunque almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione: ciò per quanto riguarda l'ambito di trattamento consentito sia ai singoli incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.

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.

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 l'Ente si è dotato di idonei strumenti elettronici e programmi che il Decreto Legislativo n. 196/2003 imporrebbe di aggiornare con cadenza almeno semestrale, ma che, in relazione al continuo evolversi dei virus, si è ritenuto opportuno di sottoporre ad aggiornamento, di regola giornalmente.

Tutti gli incaricati sono stati 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.

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 ricompresi tra i firewall e i sistemi di autenticazione.
Il terzo aspetto riguarda l'utilizzo di appositi programmi (aggiornamenti di sistemi operativi) 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.
Le misure logiche di sicurezza, di cui è dotato il Titolare per la protezione dei trattamenti che avvengono con strumenti elettronici, saranno oggetto di importanti interventi futuri relativi ai sistemi di autenticazione informatica, autorizzazione, protezione e formazione, al fine di migliorare ulteriormente l'efficacia di tali misure.

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.
Per i dati trattati con strumenti elettronici sono previste procedure di back up, 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:

- settimanale il venerdì;
- incrementale giornaliero ogni giorno lavorativo della settimana;
- ogni mese viene eseguito un ulteriore salvataggio completo;
- le copie mensile/annuali vengono custodite in una cassaforte ignifuga dislocata nell'area ad accesso controllato durante l'orario di lavoro.

6. Controllo generale sullo stato della sicurezza

Al responsabile per la sicurezza, ovvero al Dirigente del Settore Servizi Finanziari e Sistemi Informativi, è affidato il compito di aggiornare le misure di sicurezza al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnologico, 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, i Responsabili e le persone da questi appositamente incaricati provvedono, 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 o 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;
- 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.