Copia

COMUNE DI FELITTO
Provincia di Salerno
Piazza Mercato C.A.P. 84055
tel. 0828.945028 fax 0828.945638
cod. fiscale 82002890653 e p. I.V.A. 00627950652

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

Deliberazione N. 24
Del 29.03.2011

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA D. LGS. 196/03 E S.M.I. APPROVAZIONE.

L'anno duemilaundici, il giorno ventinove del mese di marzo alle ore 20,30 presso la Sede Comunale in Piazza Mercato si è riunita la Giunta Comunale alla presenza di:

	PRESENTI	ASSENTI
Maurizio Caronna	X	
Francesco Caroccia	X	
Donato Di Stasi	X	
Antonio Sabetta	X	
Angelo Trotta	X	

Constatato il numero legale degli intervenuti, il Sindaco Caronna Maurizio assume la presidenza ed invita i presenti alla trattazione dell'argomento indicato in oggetto.
Partecipa il Segretario Comunale **Dr. Sergio Gargiulo**.

LA GIUNTA COMUNALE

PREMESSO

CHE l'art. 31 del D. Lgs. 196/03 e s.m.i. "Codice in materia di protezione di dati personali" stabilisce che i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, in modo di ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, 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;

CHE l'art. 33 del medesimo Decreto, precisa che i Titolari del trattamento sono tenuti ad adottare le misure minime ivi indicate;

CHE l'insieme delle misure tecniche, informatiche, organizzative per attivare il livello minimo di protezione richiesto dal citato art. 33 è stato definito dagli artt. 34-35-36 e dall'allegato B del medesimo testo normativo;

VISTO in particolare il punto n. 19 dell'allegato B, del menzionato Decreto, il quale prevede che il Titolare dei trattamenti di dati sensibili o Giudiziari entro il 31 marzo di ogni anno rediga e predisponga un apposito "Documento Programmatico sulla Sicurezza", nel quale devono essere indicati:

- ✓ L'elenco dei trattamenti di dati personali;
- ✓ La distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- ✓ L'analisi dei rischi che incombono sui dati;
- ✓ Le misure 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;
- ✓ La descrizione dei criteri e delle modalità per il ripristino delle disponibilità dei dati in seguito a distruzione o danneggiamento;
- ✓ La previsione di interventi formativi per gli incaricati del trattamento, per renderli edotti sui rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal Titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione

di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

- ✓ La descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza nel caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del Titolare;

RITENUTO di approvare il "Documento Programmatico sulla Sicurezza" previsto dall'art. 34 e dall'allegato B del D. LGS 196/2003 e s.m.i.;

VISTO che sulla proposta della presente deliberazione è stato acquisito il parere favorevole in ordine alla regolarità tecnica del responsabile del Servizio Amministrativo, ai sensi dell'art.49, D.L.vo 267/2000 e s.m.i.;

con votazione unanime

D E L I B E R A

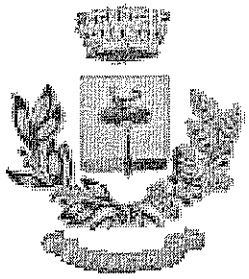
di approvare, per le motivazioni espresse in narrativa qui richiamate il "Documento Programmatico sulla Sicurezza" per l'adozione delle misure minime di sicurezza nel trattamento dei dati personali, ai sensi del decreto Legislativo 196/2003 e s.m.i.;

con successiva ed unanime votazione

D E L I B E R A

di dichiarare il presente atto immediatamente eseguibile.

COMUNE DI FELITTO
(Provincia di Salerno)



Documento Programmatico sulla Sicurezza

1. Scopo

Il presente documento programmatico sulla Sicurezza è adottato, in base alle disposizioni di cui al punto 19 del Disciplinare tecnico in materia di misure minime di Sicurezza del codice in materia di protezione dei dati personali, per definire le politiche di sicurezza in materia di trattamento di dati personali, ed i criteri organizzativi per la loro attuazione.

In particolare nel Documento Programmatico sulla Sicurezza vengono definiti i criteri tecnici organizzativi per:

a) la protezione delle aree e dei locali interessati dalle misure minime di sicurezza, nonché le procedure per controllare l'accesso alle persone autorizzate ai medesimi locali;
b) i criteri e le procedure per assicurare l'integrità dei dati;
c) i criteri e le procedure per la sicurezza della trasmissione dei dati, ivi compresi quelli per le redazioni di accesso per via telematica;
d) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

2. Campo di applicazione

Il documento Programmatico sulla Sicurezza, in raccordo con il Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. adottato dal Comune di Felitto (SA), e del quale si richiamano tutte le definizioni e disposizioni, definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.
Il documento Programmatico sulla Sicurezza riguarda tutti i dati personali:

- Sensibili
- Giudiziari
- Comuni

Si applica al trattamento di tutti i dati personali per mezzo di:

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (es. cartacei, audio, visivi e audiovisivi, ecc.)

Il Documento Programmatico sulla Sicurezza deve essere conosciuto ed applicato da tutti gli uffici del Comune di Felitto (SA).

3. Principali riferimenti legislativi

- Codice in materia di protezione dei dati personali (G.U. 29 luglio 2003, n. 174 – Supplemento ordinario n. 123/L);
- Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B D. Lgs. 196/203 e s.m.i.)

4. Composizione del documento

Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il Responsabile, se designato, un Documento Programmatico sulla Sicurezza contenente idonee informazioni riguardo:

- ✓ L'elenco dei trattamenti di dati personali;
- ✓ La distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- ✓ L'analisi dei rischi che incombono sui dati;
- ✓ Le misure 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;
- ✓ La descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- ✓ La previsione di interventi formativi degli incaricati del trattamento per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamento di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

Il Documento Programmatico sulla Sicurezza è scritto in base a quanto rilevato oggettivamente oltre che dai documenti disponibili, in conformità a quanto indicato nel Codice in materia di protezione dei dati personali.

Il Comune di Felitto (SA) è soggetto pubblico della provincia di Salerno;

- la sede principale è in Piazza Mercato n. 1 – **84055 Felitto (SA)**;

Per quanto concerne l'organizzazione interna sono individuati n. 2 Settori :

1. Settore Tecnico — Responsabile Ing. Daniele Gnazzo
2. Settore Polizia Municipale — Responsabile M.llo Parisi Giuseppe

Elenco dei trattamenti e descrizione degli strumenti utilizzati nel trattamento

(punto 19.1 allegato B D. Lgs. 196/2003)

Per ciascun trattamento effettuato, di cui si fornisce una sintetica descrizione, sono indicati:

a) le categorie di soggetti cui si riferisce (clienti, fornitori, utenti, pazienti, personale dipendente e tutti i tipi di collaboratori);
b) i tipi di dati personali trattati in base alla loro natura (giudiziari o sensibili). Laddove non sia indicato alcunché deve intendersi che il trattamento ha ad oggetto dati personali;
c) la struttura di riferimento e le altre strutture, esterne o interne, che concorrono al trattamento;
d) la tipologia di strumenti elettronici impiegati e di interconnessione.

Banca dati	Ufficio interessato	Tipologia di dispositivi di accesso
Gestione dei verbali di deliberazioni di Giunta e Consiglio	Ufficio Segreteria	Personal computer collegati in una rete locale e ad internet Archivio a Mobile
Gestione dati contenziosi		
Gestione dei Contratti		
Attività di Informazioni degli uffici		
Gestione dati Amministratori comunali		
Attività di gestione di violazioni e contestazioni al codice della strada	Ufficio di PM	Personal computer collegati in una rete locale e ad internet Archivio a Mobile
Attività di polizia giudiziaria		
Attività di gestione del commercio		
Attività di gestione dei servizi scolatici (mensa e trasporto)		
Attività di gestione pubblici esercizi		
Gestione delle Determinazioni P.M		
Attività di gestione dei servizi cimiteriali		
Attività pratiche di edilizia pubblica e privata	Ufficio Tecnico	Personal computer collegati in una rete locale e ad internet Archivio a Mobile
Gestione delle concessioni edilizie		
Gestione pratiche di condono edilizio		
Attività di vigilanza in materia ambientale		
Gestione delle Determinazioni U.T.		
Attività di gestione degli immobili comunali		

Gestione decreti di espropriazione Gestione dei lavori pubblici Attività di incarichi di progettazioni Gestione della Protezione civile Gestione dello Sportello unico Ricerca fonti di finanziamento OO.PP.	Ufficio Tecnico	Personal computer collegati in una rete locale e ad internet Archivio a Mobile
Gestione Albo pretorio on-line Attività di gestione manutenzione patrimonio Attività di gestione della rete idrica Attività di gestione dei rifiuti	Ufficio Tecnico	Personal computer collegati in una rete locale e ad internet Archivio a Mobile

Elenco dei trattamenti (informazioni essenziali)

(punto 19.1 allegato B D. Lgs. 196/2003)

Descrizione del trattamento	Categorie interessate	Natura S / G	Struttura di riferimento	Altre strutture	Descrizioni strumentali
Gestione dei verbali di deliberazioni di Giunta e Consiglio	dipendenti		Ufficio segreteria	Uffici pubblici	PC collegati in una rete locale e Internet
Gestione delle Determinazioni P.M.	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio P.M.	Uffici pubblici	PC collegati in una rete locale e Internet
Gestione delle Determinazioni U.T.	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio Tecnico	Uffici pubblici	PC collegati in una rete locale e Internet
Gestione dati contenziosi	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio segreteria	Uffici pubblici	PC collegati in una rete locale e Internet
Gestione dei Contratti	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio segreteria	Uffici pubblici	PC collegati in una rete locale e Internet
Gestione Albo pretorio on-line	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio Tecnico	Uffici pubblici	PC collegati in una rete locale e Internet
Attività di Informazioni degli uffici	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio segreteria	Uffici pubblici	PC collegati in una rete locale e Internet
Attività di gestione degli immobili comunali	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio tecnico	Uffici pubblici	PC collegati in una rete locale e Internet
Gestione del rapporto di lavoro del personale comunale impiegato a vario titolo	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio segreteria	Uffici pubblici	PC collegati in una rete locale e Internet
Gestione dati Amministratori comunali	Clienti, utenti,			Uffici pubblici	

	dipendenti e/o collaboratori, fornitori ecc.		Ufficio segreteria		PC collegati in una rete locale e Internet
Gestione del rapporto giuridico ed economico del personale	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio segreteria	Uffici pubblici	PC collegati in una rete locale e Internet
Attività di gestione di violazioni e contestazioni al codice della strada	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio di PM	Uffici pubblici	PC collegati in una rete locale e Internet
Attività di polizia giudiziaria	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio di PM	Uffici pubblici	PC collegati in una rete locale e Internet
Attività di gestione del commercio	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio di PM	Uffici pubblici	PC collegati in una rete locale e Internet
Attività di gestione pubblici esercizi	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio di PM	Uffici pubblici	PC collegati in una rete locale e Internet
Attività pratiche di edilizia pubblica e privata	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio Tecnico	Uffici pubblici	PC collegati in una rete locale e Internet
Gestione delle concessioni edilizie	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio Tecnico	Uffici pubblici	PC collegati in una rete locale e Internet
Gestione pratiche di condono edilizio	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio Tecnico	Uffici pubblici	PC collegati in una rete locale e Internet
Attività di vigilanza in materia ambientale	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio Tecnico	Uffici pubblici	PC collegati in una rete locale e Internet
Gestione decreti di espropriazione	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio Tecnico	Uffici pubblici	PC collegati in una rete locale e Internet
Gestione dei lavori pubblici	Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.		Ufficio Tecnico	Uffici pubblici	PC collegati in una rete locale e Internet

Attività di incarichi di progettazioni	**Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.**		**Ufficio Tecnico**	**Uffici pubblici**	**PC collegati in una rete locale e Internet**
Gestione della Protezione civile	**Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.**		**Ufficio Tecnico**	**Uffici pubblici**	**PC collegati in una rete locale e Internet**
Gestione dello Sportello unico	**Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.**		**Ufficio Tecnico**	**Uffici pubblici**	**PC collegati in una rete locale e Internet**
Ricerca fonti di finanziamento OO.PP.	**Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.**		**Ufficio Tecnico**	**Uffici pubblici**	**PC collegati in una rete locale e Internet**
Attività di gestione dei servizi scolatici (mensa e trasporto)	**Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.**		**Ufficio di PM**	**Uffici pubblici**	**PC collegati in una rete locale e Internet**
Attività di gestione manutenzione patrimonio	**Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.**		**Ufficio Tecnico**	**Uffici pubblici**	**PC collegati in una rete locale e Internet**
Attività di gestione della rete idrica	**Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.**		**Ufficio Tecnico**	**Uffici pubblici**	**PC collegati in una rete locale e Internet**
Attività di gestione dei rifiuti	**Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.**		**Ufficio Tecnico**	**Uffici pubblici**	**PC collegati in una rete locale e Internet**
Attività di gestione dei servizi cimiteriali	**Clienti, utenti, dipendenti e/o collaboratori, fornitori ecc.**		**Ufficio P.M.**	**Uffici pubblici**	**PC collegati in una rete locale e Internet**

Al fine di recepire completamente lo spirito con cui è stato varato il CODICE, il COMUNE DI FELITTO ha elaborato il seguente Documento Programmatico Sulla Sicurezza (nel seguito denominato più semplicemente DPSS), che testimonia lo sforzo fatto dall'Ente al fine di garantire la protezione, l'integrità, la conservazione di ogni singolo dato personale trattato.

Il documento parte innanzitutto dalla **Identificazione delle Risorse da proteggere**, risorse che hanno impatti con i problemi di sicurezza e svolgono un ruolo significativo nei processi di trattamento dei dati personali. L'**analisi dei Rischi** costituisce un punto fondamentale per affrontare in maniera definita e controllata le problematiche di sicurezza; rappresenta l'attività di raccolta ed analisi delle debolezze e lacune del rispetto del Codice all'interno dell'Ente. Successivamente all'analisi dei Rischi, si sono definite le **misure di sicurezza** (organizzative, fisiche e logiche) adottate per tutelare le strutture e le risorse preposte al trattamento dati e quindi ai dati stessi.

Vengono successivamente elencati **i criteri e le modalità per il ripristino dei dati** in caso di perdita dei dati dovuta, ad esempio, ad un guasto.

E' previsto un **Piano di Formazione degli Incaricati** per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni al sistema di elaborazione e gestione logica dei dati.

5. Compiti delle singole figure a protezione dei dati personali

Nella sezione sopra riportata sono individuati gli uffici preposti al trattamento dei dati nonché l'elenco dei dati gestiti. Al vertice di ciascun ufficio c'è il Responsabile del trattamento dei dati che coincide con il Responsabile del Settore. Gli incaricati del trattamento dei dati sono i dipendenti assegnati a ciascun settore.
Il Comune di Felitto (SA), come titolare, e le figure individuate come Responsabili ed incaricati, assicureranno che il programma di sicurezza sia adeguatamente sviluppato, realizzato e mantenuto aggiornato e conforme alla legge sulla privacy e alle prescrizioni del presente documento.

Essi, nell'ambito della propria organizzazione, opereranno in modo da:

- Minimizzare la probabilità di appropriazione, danneggiamento o distruzione anche non voluta di apparecchiature informatiche o archivi informatici o cartacei contenenti dati personali;
- Minimizzare la probabilità di accesso, comunicazione o modifiche non autorizzate alle informazioni personali;
- Minimizzare la probabilità che i trattamenti dei dati personali siano modificati senza autorizzazione.

5.1 Il Titolare del trattamento

Tra i compiti che la Legge assegna al Titolare e che non sono delegabili, è prevista la vigilanza sul rispetto da parte dei Responsabili delle proprie istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

5.2 Il Responsabile del Trattamento dei dati personali

Sono considerati Responsabili del trattamento dei dati personali del Comune di Felitto (SA) i Responsabili di ciascun settore secondo l'articolazione organizzativa dell'ente, ciascuno per il settore di competenza, che per esperienza, capacità e affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, compreso il rifilo della sicurezza.

Il Responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le seguenti responsabilità:

- Promuovere lo sviluppo, la realizzazione ed il mantenimento dei programmi di sicurezza contenuti nel presente Documento Programmatico sulla Sicurezza dei dati personali;
- Informare il Titolare del trattamento sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti;
- Promuovere lo svolgimento di un continuo programma di addestramento degli Incaricati del Trattamento e mantenere attivo un programma di controllo della corrispondenza con le regole di sicurezza.

5.3 Gli incaricati del trattamento

Gli incaricati del trattamento dei dati personali, con specifico riferimento alla sicurezza, hanno le seguenti responsabilità:

- Svolgere attività previste dai trattamenti secondo el prescrizioni contenute nel presente Documento Programmatico sull Sicurezza e le direttive del Responsabile.
- Non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del Responsabile del trattamento;
- Rispettare e fari rispettare le norme di sicurezza per la protezione dei dati personali;
- Informare il Responsabile in caso di incidente di sicurezza che coinvolga dati personali.

6. Analisi dei rischi

Il D. lgs. 196/2003 ha per finalità quella di garantire che "il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".

Sulla base di quanto prescritto da tale Codice, vengono individuati tre requisiti di sicurezza, che costituiscono il riferimento per valutare il proprio grado di corrispondenza rispetto a quanto indicato dal D. lgs. 196/2003.

I tre requisiti sono:

riservatezza: requisito specificatamente indicato nelle finalità del CODICE, si riferisce alla possibilità di intraprendere azioni in grado di proteggere i dati di natura personale e sensibile da modalità di trattamento non autorizzato che contemplano il rischio di accesso ai dati, e rientranti nelle seguenti categorie di attività specificatamente indicate dalla legge:

- raccolta,
- registrazione,
- organizzazione,
- conservazione,
- comunicazione,
- diffusione,
- selezione,
- estrazione,
- raffronto,
- interconnessione,
- utilizzo

integrità: tale requisito si riferisce alla possibilità di intraprendere azioni in grado di proteggere i dati di natura personale e sensibile da modalità di trattamento non autorizzate che contemplano il rischio di modifica delle informazioni, e rientranti nelle seguenti categorie di attività specificatamente indicate dalla Legge:

- elaborazione,
- modificazione,
- cancellazione,

- blocco,
- distruzione

disponibilità: tale requisito si riferisce alla necessità di intraprendere azioni in grado di proteggere dati di natura personale e sensibile, da possibili eventi che possono ridurre la capacità dell'azienda di assolvere alle finalità di trattamento per cui tali dati sono stati raccolti.

Tali requisiti forniscono quindi un punto di partenza per l'identificazione dei possibili attacchi, individuabili in base all'analisi dello scenario effettuata, e servono alla definizione dei criteri di protezione più adeguati a garantire tale necessità di protezione.

Per Analisi dei Rischi si intende l'attività di raccolta ed analisi delle minacce e delle vulnerabilità a cui sono soggette le risorse nel rispetto del CODICE.
Per ciascun dato è quindi necessario individuare ed analizzare i relativi rischi, anche accidentali.
Gli indici di rischio sono fissati mediante una scala semiqualitativa a 3 valori riportatati nella successiva tabella.

Livello criticità	Descrizione
2	Rischio molto basso: identifica una minaccia remota e comunque rapidamente reversibile od ovviabile.
1	Rischio medio: superiore al precedente identificante una minaccia remota ma i cui effetti non sono totalmente o parzialmente reversibili od ovviabili. In tale caso è già consigliabile pensare ad accorgimenti per contenere il rischio.
0	Rischio alto: vengono individuati rischi che è sicuramente inaccettabile pensare di correre. Pertanto dovrà sicuramente essere attivato un insieme di contromisure (di natura fisica, logica, etc..) per abbattere il rischio e contenerlo in livelli accettabili.

6.1 Analisi dei rischi sui luoghi fisici

Controllo	Sede	Livello criticità	Misure adottate
Possibilità di intrusione / Furto	MUNICIPIO	2	Durante il normale svolgimento dell'attività lavorativa i locali sono presidiati dai dipendenti addetti. Al termine dell'orario di lavoro, l'ingresso viene chiuso a chiave e i locali **non sono** protetti da un impianto d'allarme. Le finestre degli uffici ubicati al piano terra sono dotate di inferriate.
	POLIZIA MUNICIPALE	2	Durante il normale svolgimento dell'attività lavorativa, i locali non sono sempre presidiati dai dipendenti addetti in quanto questi sono spesso sul territorio. Al termine dell'orario di lavoro, l'ingresso viene chiuso a chiave e i locali **non sono** protetti da un impianto d'allarme. I locali sono ubicati al piano terra.
Allagamenti	TUTTE LE SEDI	2	Non tutti gli elaboratori client sono sollevati da terra. Il server è sollevato da terra.
Incendio	MUNICIPIO ARCHIVIO COMUNALE POLIZIA MUNICIPALE	1	I locali sono dotati di un idoneo numero di estintori.
Climatizzazione	MUNICIPIO	2	La sala server non è dotata di impianto di condizionamento ambientale così come anche alcuni gli uffici della casa comunale e della sede dell'archivio. La sala server è dotata di impianto elettrico a norma, porta chiudibile a chiave e gruppo di continuità che permette il salvataggio in caso di black out.
Impossibilità di rilevare accessi non autorizzati	TUTTE LE SEDI		Le sedi sono costantemente presidiate dai dipendenti durante il normale svolgimento dell'attività lavorativa ad eccezione della sede dell'Archivio.

6.2 Analisi dei rischi sule risorse hardware

Controllo	Sede	Livello criticità	Misure adottate
Uso non autorizzato dell'hardware	TUTTE LE SEDI	2	L'utilizzo dell'hardware è soggetto all'utilizzo di password
Manomissione/sabotaggio	TUTTE LE SEDI	2	Alle risorse non accedono persone non autorizzate. La manutenzione è effettuata da tecnici di fiducia.
Probabilità/frequenza di guasto	TUTTE LE SEDI	2	L'hardware acquistato è di qualità e storicamente non ha mai dato problemi rilevanti.
Rischi connessi all'elettricità.	MUNICIPIO	0	Non tutti gli elaboratori sono collegati ad un gruppo di continuità che fornisce energia e impedisce l'improvvisa assenza di corrente elettrica.

6.3 Analisi dei rischi sule risorse software

Controllo	Sede	Livello criticità	Misure adottate
Accesso non autorizzato alle basi dati connesse	TUTTE LE SEDI	2	I software che trattano i dati controllano l'accesso tramite una finestra di autenticazione (finestra di Login).
Errori software che minacciano l'integrità dei dati	TUTTE LE SEDI	2	I software sono utilizzati da parecchi anni e non hanno mai causato la perdita o il danneggiamento dei dati trattati
Presenza di codice non conforme alle specifiche del programma	TUTTE LE SEDI	2	I programmi sono forniti da produttori che operano nel settore con la massima serietà da molti anni.
Aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti	TUTTE LE SEDI	2	I programmi vengono aggiornati periodicamente.

6.4 Analisi dei rischi sulle risorse dati

Accesso non autorizzato	TUTTE LE SEDI	2	L'accesso alle risorse dati in formato elettronico avviene solo tramite gli elaboratori protetti da password. Ai documenti cartacei possono accedere solo i diretti incaricati.
Cancellazione non autorizzata di dati / manomissione di dati	TUTTE LE SEDI	2	L'accesso agli elaboratori avviene solo tramite gli elaboratori protetti da password. Ai documenti cartacei possono accedere solo i diretti incaricati.
Perdita di dati	TUTTE LE SEDI	2	Il server ha una alta affidabilità. Sono effettuate periodiche copie di backup.
Backup dei dati	TUTTE LE SEDI	2	Il backup dei dati viene eseguito periodicamente.
Protezione da virus	TUTTE LE SEDI	2	Presente il software antivirus aggiornato periodicamente.

I locali e i contenitori nei quali sono archiviati o dai quali è possibile l'accesso ai dati devono essere sempre presidiati da personale autorizzato. In caso di assenza, anche temporanea, di idoneo presidio i locali e i contenitori dei dati devono essere debitamente resi inaccessibili attivando i sistemi di chiusura disponibili. Qualora le chiusure siano deteriorate o mancanti è compito del Responsabile dell'ufficio dare immediata comunicazione all'ufficio preposto alla manutenzione degli immobili. La gestione delle chiavi di accesso ai contenitori dei dati o all'ufficio, qualora detti contenitori ne fossero sprovvisti, deve essere effettuata a cura del Responsabile dell'ufficio che provvederà a gestire un elenco di tutti i deterntori delle chiavi e a mantenerlo aggiornato.

I Responsabili dei vari settori devono mantenere un effettivo controllo sull'area di sua responsbilità.
Le persone autorizzate ad accedere sono esclusivamente gli incaricati o i responsabili dei trattamenti dei dati.
I visitatori occasionali dovono essere accompagnati.
Gli ingressi fuori orario devono essere autorizzati e controllati.

L'accesso alla sala server è limitato ai soli addetti al sistema informativo o alle persone espressamente autorizzate dagli stessi, per il tempo strettamente necessario allo svolgimento dei compiti eventualmente assegnati (es. Manutenzione software e/o ardware di un server).
In assenza di personale autorizzato, la sala server viene mantenuta chiusa a chiave.
I supporti di back up vengono conservati in cassaforte situata nell'ufficio anagrafe.
I locali nei quali sono archiviati dati personali devono essere sempre presidiati da parsonale autorizzato. In caso di assenza, anche temporanea (es. Durante la pausa pranzo), del personale incaricato dei trattamenti dei dati, i locali e i contenitori dei dati dovono essere resi inaccessibili attivando i sistemi di chiusura disponibili. Qualora le chiusure siano deteriorate o mancanti il Responsabile del trattamento dei dati e gli incaricati del trattamento dei dati dell'ufficio sono tenuti a dare immediata comunicazione all'ufficio preposto alla manutenzione degli immobili.

Gli incaricati sono tenuti a fine giornata a non lasciare sulla scrivania e a riportare negli armadi tutta la documentazione contenente dati personali. I dati sensibili dovono essere riposti negli armadi chiusi a chiave e conservati separatamente dagli altri dati personali.

7. Quadro riassuntivo delle misure volte a controllare l'accesso ai locali interessati dalle misure di sicurezza

Tipo di misura	Misura
Fisica	Impianto elettrico a norma
Fisica	Estintori in ogni piano della sede comunale
Fisica	Porte chiudibili a chiave per tutti gli uffici
Fisica	Conservazione dei dati personali negli armadi, fuori dagli orari di ufficio, necessariamente chiusi a chiave per la conservazione dei dati sensibili.

8. Quadro riassuntivo delle misure volte ad assicurare l'integrità dei dati

Tipo di misura	Misura
Fisico	Gruppo statico di continuità per supporto al server di rete
Fisico	Utilizzo di password su ogni stazione di lavoro
Fisica / logica	Gestione delle connessioni con l'esterno
Organizzativa	Backup
Organizzativa	Conservazione in luoghi sicuri delle diverse copie di backup
Organizzativa	Cancellazione di supporti informatici contenenti dati sensibili o giudiziari non più necessari
Organizzativa / logica	Tutti gli utilizzatori non devono lasciare incustodito il PC. A tal fine predisporre lo screensaver automatico, dopo pochi minuti di inutilizzo. Il riutilizzo del PC deve richiedere l'immissione delle credenziali (UsedID e Password)
Logica	Dotare ogni PC e Server di dispositivo antivirus ed aggiornarlo periodicamente
Organizzativa	Eseguire un'adeguata informazione /formazione del personale incaricato nella gestione del sistema della privacy; ricordandogli che essi hanno accesso ai soli dati personali e/o sensibili, la cui conoscenza è strettamente necessaria per adempiere ai compiti loro affidati

9. Criteri e modalità per il ripristino della disponibilità dei dati

Al fine di assicurare il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento ed impedirne la comunicazione e/o diffusione non autorizzata, il COMUNE DI FELITTO (SA) ha elaborato i seguenti criteri e modalità.

Salvataggio regolare dei dati

Il salvataggio dei dati è una procedura che ricopre una funzione cruciale. Attraverso questa procedura, è possibile, in caso di guasto hardware dei dischi, "ripristinare" il sistema nello stesso stato in cui si trovava nel momento dell'ultimo salvataggio.
Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza giornaliera.

Criteri per l'eliminazione dei supporti di memorizzazione obsoleti

I supporti rimovibili, se non utilizzati, sono distrutti o resi inutilizzabili.
Possono essere riutilizzati da altri incaricati se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

Misure per la custodia dei supporti di memorizzazione.

I supporti di memorizzazione utilizzati per l'attività di backup sono conservati in armadi ignifughi posti in locali distanti dalla sala server.

10. Piano di formazione del personale autorizzato al trattamento dei dati

Attualmente il COMUNE DI FELITTO ha previsto incontri formativi di sensibilizzazione, informazione e aggiornamento ai dirigenti, responsabili e incaricati sulla corretta modalità operativa per il trattamento dei dati e sui nuovi strumenti e /o misure di sicurezza implementati in azienda.
In particolare, sono stati previsti due moduli formativi:
Giugno 2011 e Dicembre 2011 presso corsi formativi eseguiti da Enti e/o società accreditate.

Coerentemente con l'evoluzione degli strumenti tecnici adottati dal COMUNE DI FELITTO (SA) e/o all'insorgere di nuove disposizioni legislative in materia, nonché al momento dell'ingresso in servizio o in occasione di cambiamenti di mansioni, verranno istituiti nuovi incontri formativi. In ogni caso, almeno una volta l'anno, verrà comunque istituito un incontro per risensibilizzare gli incaricati sull'importanza di adottare le norme di sicurezza predisposte e per recepire eventuali suggerimenti in materia derivanti dalla constatazione della presenza di minacce o vulnerabilità riscontrate.

11. Periodicità di revisione del documento programmatico sulla sicurezza

Il Documento Programmatico Sulla Sicurezza deve essere sottoposto a revisione e aggiornato entro il 31 marzo di ogni anno. Trascorso tale termine deve essere oggetto di revisione per adeguarlo ad eventuali variazioni del livello di rischio a cui sono soggetti i dati personali e ad eventuali modifiche della tecnologia informatica.
Nell'attesa dell'adeguamento conservano validità le regole in vigore.

12.Trattamenti affidati all'esterno

In caso di trattamenti di dati affidati, in conformità al codice, all'esterno della struttura del titolare è necessario che il soggetto a cui viene affidato il trattamento si assuma alcuni impegni su base contrattuale.
Pertanto il soggetto cui le attività sono affidate deve dichiarare:

- di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali, sono soggetti all'applicazione del codice per la protezione dei dati personali;
- di ottemperare agli obblighi previsti dal codice per la protezione dei dati personali;
- di impegnarsi ad avvisare immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
- di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

Conclusioni
Qualsiasi abuso dei dati gestiti o che comunque si rendono accessibili tramite le strutture dell'ente deve essere immediatamente comunicato al Responsabile del trattamento.

Approvato e sottoscritto

IL SEGRETARIO COMUNALE
F/to: Dr Sergio Gargiulo

IL SINDACO
F/to: Maurizio Caronna

COPIA conforme all'originale, in carta libera, per uso amministrativo

COMUNE DI TELESE (Salerno)

Il Segretario Comunale
Dr. Sergio Gargiulo

Ai sensi e per gli effetti dell'art. 49 del D. Lgs. 18 agosto 2000 n. 267 sulla proposta di deliberazione viene espresso il parere favorevole in merito alla regolarità tecnica da:

Il Responsabile del Servizio
F/to: Rag. Vito Galzerano

Il sottoscritto Segretario Comunale, visti gli atti d'ufficio

ATTESTA

che la presente deliberazione:

E' stata pubblicata all'Albo Pretorio Comunale on-line per quindici giorni consecutivi dal 03 MAG. 2011 al _____ come prescritto dall'art. 32, comma 1, della L. 69/2009 e dall'art. 124, comma 1, del T.U. N.267/2000;

E' stata comunicata con lettera n._____ in data _____ ai signori Capi Gruppo Consiliari, come prescritto dall'art.125, del T.U. N.267/2000;

Si certifica altresì che la presente delibera è divenuta esecutiva il giorno _____ decorsi 10 giorni dalla pubblicazione ed è stata pubblicata fino al _____

Dalla residenza Municipale

IL SEGRETARIO COMUNALE