COMUNE DI
COMO
Servizio Archivio e
Protocollo

Manuale per la gestione
del protocollo, dei flussi documentali e degli archivi

(Artt. 3 e 5 DPCM 31 ottobre 2000)

Allegato n. 8
Documento programmatico per la sicurezza
per il trattamento dei dati personali
all'interno dell'Ente - Piano per la sicurezza informatica

(deliberazione della Giunta Comunale n. 81 del 25 marzo 2013).

COMUNE DI COMO

DELIBERAZIONE DELLA GIUNTA COMUNALE

N. **81** di Registro

SEDUTA DEL 25 Marzo 2013

PRESIDENTE: DOTT. MARIO LUCINI

VICE SEGRETARIO GENERALE VICARIO: AVV. MARINA CERESA

Sono presenti al momento della votazione della seguente deliberazione:

		PRESENTI	ASSENTI
LUCINI MARIO	Sindaco	si	
MAGNI SILVIA	Vice Sindaco	si	
IANTORNO MARCELLO	Assessore	si	
CAVADINI LUIGI	“	si	
INTROZZI GISELLA	“	si	
MAGATTI BRUNO	“	si	
SPALLINO LORENZO	“	si	
PUSTERLA GIULIA	“	si	
GEROSA DANIELA	“	si	

OGGETTO: AGGIORNAMENTO DOCUMENTO PROGRAMMATICO SULLA SICUREZZA - ANNO 2013

LA GIUNTA COMUNALE

Premesso che:

- l'articolo 31, del D.Lgs. 196/03, "Codice in materia di protezione dei 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, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da 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;

- l'articolo 33 del D. Lgs. 196/03 precisa che i Titolari di trattamento sono comunque tenuti ad adottare le misure minime ivi indicate o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali;

- le misure tecniche, informatiche, organizzative per attivare il livello minimo di protezione richiesto dall'articolo 33 sono state definite nei successivi articoli 34-35-36 e nell'allegato B del "Codice" e dato atto che le stesse sono aggiornate periodicamente con Decreto interministeriale ai sensi del citato art. 36;

- con provvedimento del 27 novembre 2008, pubblicato in G.U. n. 300 del 24 dicembre 2008, il Garante ha emanato le "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";

- con Provvedimento del 25 giugno 2009, pubblicato in G.U. n. 149 del 30 giugno 2009, il Garante ha apportato modifiche al provvedimento del 27.11.2008;

- con l'articolo 14, comma 1, la Legge n. 183 del 4.11.2010, ha modificato la disciplina del trattamento di dati personali effettuato da soggetti pubblici prevista dal Codice in materia di protezione dei dati personali;

Rilevato che l'articolo 34 del D.Lgs. 196/03 prevede in particolare per il trattamento di dati personali effettuato con strumenti elettronici l'obbligo delle tenuta di un aggiornato documento programmatico sulla sicurezza dei dati;

Vista la regola 19 dell'allegato B D.Lgs. 193/03 che prevede che il "DOCUMENTO PROGRAMMATICO SULLA SICUREZZA" sia redatto entro il 31 marzo di ogni anno e che in esso siano contenuti:

1. l'elenco dei trattamenti di dati personali;
2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
3. l'analisi dei rischi che incombono sui dati;
4. 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;
5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento ;

6. 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 cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Atteso che il Comune di Como effettua trattamenti dei dati sensibili o giudiziari di cui agli articoli 20 – 21 – 22 del D. Lgs. N. 196/2003 per lo svolgimento delle proprie finalità istituzionali;

Richiamata la propria deliberazione n. 308 del 9.11.2005 con cui si è proceduto, per la prima volta, all'approvazione del Documento Programmatico sulla sicurezza e si è previsto, in attuazione della Regola 19 dell'allegato B del "Codice in materia di protezione dei dati personali" che il DPS fosse aggiornato annualmente;

Visto il Regolamento per il trattamento dei dati sensibili e giudiziari, approvato con delibera del Consiglio Comunale n. 25 del 20.3.2006;

Ritenuta la propria competenza ai sensi dell'art. 48 del T.U.EE.LL.;

Visto il parere favorevole espresso sulla proposta di deliberazione, ai sensi dell'art. 49, 1° comma, del D.Lgs. n. 267/2000 dal Dirigente del Settore Sistemi Informativi, Programmazione e Controllo di Gestione;

Visto, altresì, il parere favorevole espresso sulla proposta di deliberazione dal Segretario Generale ai sensi dell'art. 134, 2° comma, dello Statuto Comunale;

Ad unanimità di voti espressi nei modi di legge:

D E L I B E R A

1°) di approvare l'unito aggiornamento del Documento Programmatico sulla Sicurezza.

Letto, approvato e sottoscritto.

IL VICE SEGRETARIO GENERALE VICARIO	IL PRESIDENTE
AVV. MARINA CERESA	DOTT. MARIO LUCINI

Il sottoscritto VICE SEGRETARIO GENERALE VICARIO, visti gli atti d'ufficio

A T T E S T A

che la presente deliberazione:

- è stata pubblicata all'Albo Pretorio per 15 giorni consecutivi dal ai sensi dell'art. 124, 1° comma, del D.Lgs. 18/08/2000 n. 267 ed in pari data è stata comunicata ai Capigruppo Consiliari, così come prescritto dall'art. 125 dello stesso Decreto;

☐ è stata adottata in via d'urgenza, ai sensi dell'art. 42, 4° comma, del D.Lgs. 267/2000;

☐ è esecutiva ai sensi dell'art. 134, 4° comma, del D.Lgs. n. 267/2000;

☐ è divenuta esecutiva decorsi 10 giorni dalla pubblicazione (art. 134, 3° comma, del D.Lgs. n. 267/2000).

Como, ……

IL VICE SEGRETARIO GENERALE VICARIO

.....

Documento Programmatico sulla Sicurezza

Aggiornamento anno 2013

Comune di Como

Sommario

Indice Tabelle

1. PREMESSA

Con Decreto Legislativo 30.6.2003 n. 196 è stato approvato il "Codice in materia di protezione dei dati personali" che ha abrogato la legge 31.12.1996 n. 675 e successive modifiche ed integrazioni.
Dal primo gennaio 2004 è entrato in vigore il nuovo Codice (D.Lgs.196/2003) in materia di protezione dei dati personali. L'obbligatorietà dell'adeguamento alla nuova normativa coinvolge tutti coloro che per l'espletamento della loro attività trattano dati personali.
Con provvedimento del 27 novembre 2008, pubblicato in G.U. n. 300 del 24 dicembre 2008, il Garante ha emanato le "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", modificato con Provvedimento del 25 giugno 2009.
Gli interventi da attuare possono riassumersi nella nomina di un titolare e di responsabili per la gestione della protezione dei dati, la chiara identificazione di tutti gli incaricati del trattamento, la messa in sicurezza degli elaboratori utilizzati per il trattamento dei dati contro ogni possibile violazione o inficiamento del funzionamento, nella trascrizione delle procedure interne da seguire e nella redazione di un Documento Programmatico sulla Sicurezza (DPS) aggiornato con cadenza annuale. Il DPS costituisce l'elemento di prova dell'adeguamento dell'Ente alla nuova normativa.
Particolarmente importante, nel Codice, è l'estensione delle misure minime di sicurezza non solo alle aziende che per la propria attività devono trattare dati sensibili, ma a tutte quelle realtà nelle quali viene effettuata l'archiviazione informatica di dati personali di fornitori, clienti, dipendenti e quant'altro. Vige pertanto un obbligo di adozione di misure minime di sicurezza ossia quel complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione normativamente richiesto rispetto ai rischi di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
Nel segnalare a tutti i titolari di trattamenti di dati personali soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici la particolare criticità del ruolo degli amministratori di sistema, il Garante, ai sensi dell'art. 154, comma 1, lett. h) del Codice, richiama l'attenzione dei Titolari sull'esigenza di valutare con particolare attenzione l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema (*system administrator*), amministratore di base di dati (*database administrator*) o amministratore di rete (*network administrator*), laddove tali funzioni siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali, , tenendo ovviamente in considerazione l'opportunità o meno di tale attribuzione e le concrete modalità sulla base delle quali si svolge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato.
Con il provvedimento del 27 novembre 2008, il Garante ha introdotto un nuovo adempimento in materia di gestione e protezione dei dati personali trattati attraverso sistemi informatici e di garanzia alla sicurezza degli stessi dati e sistemi. Si tratta dell'obbligo per gli amministratori di sistema (compresi coloro che svolgono la mansione di amministratore di rete, di data base o i manutentori), di conservare gli "access log" per almeno sei mesi in archivi immodificabili e inalterabili. Devono, cioè, essere adottati sistemi idonei alla registrazione degli accessi logici, ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema e, novità forse più importante, gli access log devono avere le caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste; ciò vuol dire che le registrazioni devono avere i riferimenti temporali certi e la descrizione

dell'evento che le ha generate e devono essere conservate per un congruo periodo (non inferiore a sei mesi).
Per rispondere al nuovo adempimento, con determina dirigenziale n.89/1781 R.G. del 20.11.2009, è stato acquistato dalla ditta Know-it di Milano un sistema che consente la registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione ed agli archivi elettronici, adeguando così l'Ente alle previsioni contenute nella misura f) del Provvedimento del Garante del 27/11/2008.
Il Codice prevede inoltre l'obbligatorietà della formazione al personale incaricato del trattamento dei dati e la sua pianificazione fin dal momento dell'assunzione di nuovi elementi di staff. Questo aspetto è di particolare importanza per garantire il corretto rispetto della normativa nonché prevenire inconvenienti quotidiani che possono derivare da un uso improprio delle apparecchiature informatiche da parte di personale non specializzato.

1.1 PRINCIPI GENERALI

L'Ente comune di Como, come Titolare del trattamento dei dati personali, assicura che il programma di sicurezza sia adeguatamente sviluppato, realizzato e mantenuto aggiornato e conforme alla legge sulla privacy e alle prescrizioni del presente documento.
L'Ente, nell'ambito della propria organizzazione, opera 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,
- accesso, comunicazione o modifiche non autorizzate alle informazioni personali,
- modifica senza autorizzazione dei trattamenti dei dati personali.

1.2 APPLICABILITÀ

Il presente Documento Programmatico sulla Sicurezza delle informazioni si applica a tutta la struttura informativa dell'Ente. I Responsabili incaricati dal Titolare hanno l'onere di divulgare il contenuto del presente Documento agli Incaricati e di formare il personale assegnato alla propria struttura.

1.3 REVISIONE DEL DOCUMENTO

Il presente documento è valido per un 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.

1.4 DISPOSIZIONI PER L'ESERCIZIO DELLA VIDEOSORVEGLIANZA

Per il trattamento dei dati realizzato mediante l'impianto di videosorveglianza si fa espresso rinvio all'apposito regolamento approvato dal Consiglio Comunale con delibera n. 11 del 9 marzo 2009.

2. LA PRIVACY NELLE PUBBLICHE AMMINISTRAZIONI

Sulla base di alcuni principi generali fissati dal Codice per tutti i trattamenti effettuati da soggetti pubblici e privati, le amministrazioni pubbliche sono legittimate a trattare dati personali comuni, sensibili o giudiziari soltanto per svolgere funzioni istituzionali, rispettando gli eventuali altri presupposti e limiti stabiliti da disposizioni normative estranee al Codice ed astenendosi dall'acquisire il consenso degli interessati, specie per rendere lecito un trattamento altrimenti non ammesso.
Il Codice rafforza le garanzie per i cittadini, ridefinisce la categoria dei dati giudiziari, includendovi le informazioni relative alla qualità di indagato o di imputato. In particolare, viene rafforzato e sviluppato il principio di proporzionalità nel trattamento di queste informazioni, ritenendosi legittimo il trattamento dei soli dati sensibili e giudiziari "indispensabili" allo svolgimento di attività che non potrebbero essere adempiute mediante il ricorso a dati anonimi o a dati personali di diversa natura (art. 22 d.lgs. n. 196/2003). Con questo limite, resta ferma la possibilità per i soggetti pubblici di trattare i dati sensibili o giudiziari quando ciò sia previsto da una norma di legge (oppure, se si tratta di dati giudiziari, da un provvedimento del Garante) che specifichi espressamente le rilevanti finalità di interesse pubblico perseguite, i dati personali che possono essere utilizzati e le operazioni di trattamento eseguibili (v. anche art. 27 d.lgs. n. 196/2003).
Per quanto riguarda i dati sensibili, nel caso in cui la legge (o, in via transitoria, il Garante) specifichi soltanto le finalità di rilevante interesse pubblico, il Codice conferma l'adeguata soluzione secondo cui l'atto con il quale le amministrazioni devono individuare e rendere pubblici i tipi di dati utilizzabili e le operazioni eseguibili deve avere natura regolamentare e non già meramente amministrativa (artt. 20 s. d.lgs. n. 196/2003). I regolamenti sono adottati in conformità al parere reso dal Garante, che può essere formulato anche su schemi tipo al fine di rendere più agevole e rapida l'adozione di tali atti. Qualora gli schemi regolamentari predisposti corrispondano ai modelli su cui il Garante ha reso un parere conforme, non è necessario sottoporli allo specifico esame da parte dell'Autorità.

2.1 TRASPARENZA DELL'ATTIVITÀ AMMINISTRATIVA

2.1.1 PUBBLICITÀ DELLE DELIBERAZIONI COMUNALI E DIVIETO DI DIFFUSIONE DEI DATI SULLA SALUTE

La necessità di bilanciare il principio di trasparenza dell'attività amministrativa, sancito dalla legge n. 241/1990 e da altre disposizioni di settore (per gli enti locali, cfr. l'art. 10, comma 1, del d.lgs. n. 267/2000) con quello di tutela della riservatezza continua a rappresentare una delle problematiche che più di frequente vengono sottoposte all'attenzione del Garante.
L'Autorità ha ribadito in varie occasioni che, sebbene la normativa preveda la pubblicità per le deliberazioni comunali attraverso la loro affissione all'albo pretorio, e prossimamente sul sito internet del Comune, nel caso in cui esse contengano dati sulla salute occorre tenere presente il divieto di diffusione di tali informazioni (art. 23, comma 4, legge n. 675/1996; ora, art. 22, comma 8, d.lgs. n. 196/2003). L'ente può quindi utilizzare unicamente diciture generiche, codici numerici o lettere puntate che impediscano di giungere all'identificazione dell'interessato, attraverso una nuova tecnica di redazione dei provvedimenti soggetti ad obbligatoria pubblicazione, che lascia comunque impregiudicato il diritto dei contro-interessati ad accedere in conformità ai presupposti di legge,

presso gli uffici dell'ente, ai dati sensibili (da omettere, invece, nella delibera diffusa ad un pubblico indeterminato).
Anche in riferimento ad altri momenti della vita amministrativa, le amministrazioni sono tenute in termini più generali a selezionare con particolare attenzione i dati personali, specie se di tipo sensibile o attinenti a vicende giudiziarie, la cui menzione sia effettivamente necessaria per perseguire, nei singoli casi, le finalità di trasparenza delle attività dei propri organi, nel rispetto dei principi di pertinenza e non eccedenza (art. 9 legge n. 675/1996; ora, art. 11 d.lgs. n. 196/2003).
Gli obblighi previsti in materia di informativa comportano che le amministrazioni pubbliche rendano conoscibile agli interessati, con modalità adeguate, anche il trattamento dei dati che li riguardano effettuato a fini istituzionali. In questo senso, può non contrastare con la normativa sulla protezione dei dati la verifica, per motivi di sicurezza, dell'identità delle persone che accedono ad uffici pubblici, purché sia resa l'informativa agli interessati, anche tramite modalità semplificate (ad esempio, mediante l'affissione di avvisi chiari e sintetici), e siano osservati rigorosamente i principi di pertinenza e di non eccedenza dei dati raccolti con particolare riferimento alla mera verifica dell'identità, all'annotazione degli ingressi oppure alla prassi di fotocopiare documenti.

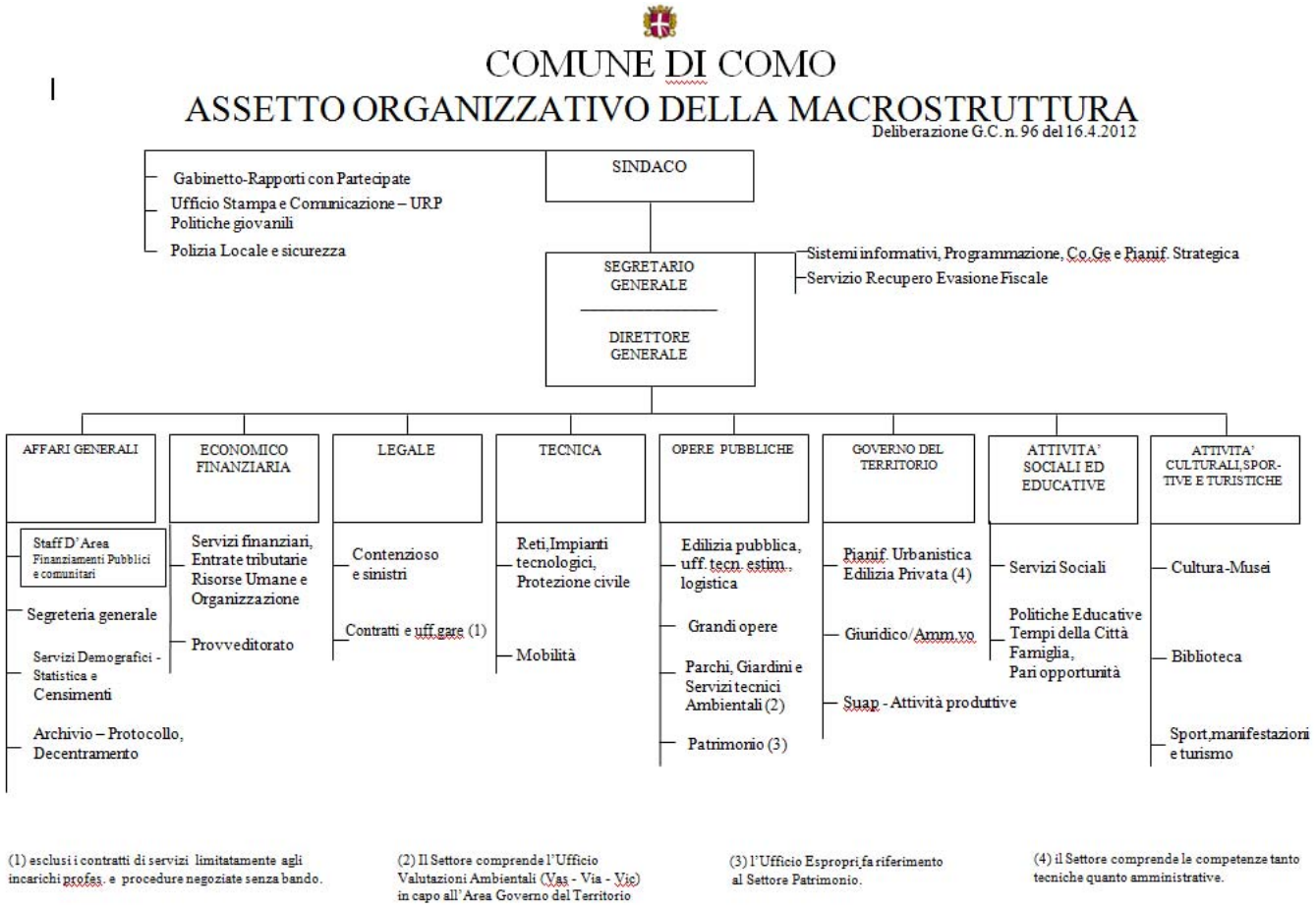
2.1.2 ACCESSO AI DOCUMENTI AMMINISTRATIVI

L'esperienza applicativa ha individuato da tempo alcuni opportuni presupposti per bilanciare il diritto alla riservatezza e il diritto di accesso ai documenti amministrativi, specie quando i documenti contengono dati attinenti alla salute o alla vita sessuale.
Con riferimento al caso in cui una pubblica amministrazione riceva una richiesta di accesso a documenti amministrativi contenenti tale tipo di dati, il Codice (art. 60), risolvendo alcuni dubbi interpretativi sorti sulla base delle disposizioni previgenti (art. 16 d.lgs. 11 maggio 1999, n. 135), dispone che il trattamento dei dati finalizzato a permettere l'accesso è consentito se la situazione giuridica che si intende tutelare con la richiesta di accesso ai documenti amministrativi è "di rango almeno pari ai diritti dell'interessato", ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile.

3. STRUTTURA ORGANIZZATIVA

3.1 L'ORGANIZZAZIONE DELL'ENTE

Di seguito si riporta l'organigramma del Comune di Como, la cui ultima variazione è stata approvata con deliberazione della Giunta Comunale n. 96 del 16 aprile 2012.



4. INDIVIDUAZIONE RISORSE

Ai fini della sicurezza le risorse identificate sono:

- gli apparati fisici e i dispositivi, direttamente coinvolti nel o a supporto del processo di elaborazione, archiviazione e trasmissione delle informazioni, il cui danneggiamento, alienazione o distruzione può provocare l'interruzione di funzionamento e la conseguente sospensione di servizio, ovvero la diffusione di informazioni;
- i sistemi operativi o i prodotti software la cui modifica, cancellazione o indisponibilità può comportare l'interruzione di funzionamento e la conseguente sospensione del servizio, ovvero la possibilità di accesso o alterazione di dati da parte di personale non autorizzato;
- il software applicativo la cui manomissione, cancellazione o indisponibilità può produrre la sospensione di alcune funzioni o l'alterazione delle corrette caratteristiche di funzionamento del Sistema Informativo;
- le informazioni (dati) la cui indisponibilità, manomissione o divulgazione può provocare la sospensione di funzioni del Sistema Informativo, compromettere il suo corretto funzionamento o procurare danno diretto o indiretto al Comune di Como.

4.1 ARCHITETTURA INFORMATICA

L'architettura del sistema informatico limitatamente alle componenti di supporto alle attività precedentemente elencate, si articola su due livelli principali e distinti :

- il livello centrale, rappresentato dal Centro Elaborazione Dati (CED) situato presso la sede centrale del municipio..
- dai sistemi informatici di produzione in dotazione al CED e dalla rete locale che connette i vari sistemi e le postazioni client di lavoro;
- gli uffici,

Il Sistema Informativo è caratterizzato da un'architettura distribuita sull'intero territorio della città di Como. Tutte le sedi informatizzate degli uffici sono dotate di reti locali LAN che connettono tutti i sistemi in esse presenti. Di seguito si riporta il disegno di rete di tale infrastruttura.

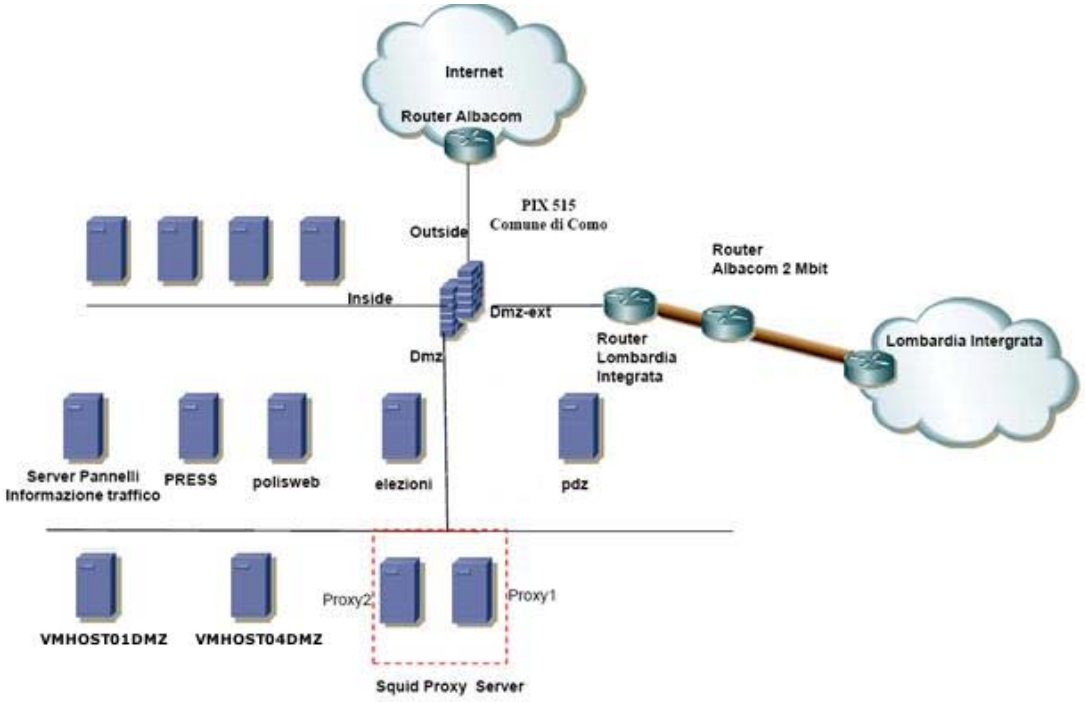


Figura 1 Infrastruttura informatica Comune di Como

Gli elementi caratterizzanti tale architettura sono i seguenti:

- vmware esxi 4.1;
- i sistemi centrali su piattaforma Windows 2008 Server che opera da server rispetto alle postazioni di lavoro;
- i sistemi centrali su piattaforma Windows 2003 Server che opera da server rispetto alle postazioni di lavoro;
- il sistema centrale su piattaforma Windows 2000 Server che opera da server rispetto alle postazioni di lavoro;
- i sistemi applicativi che assumono la funzione di server rispetto ai servizi erogati;
- le postazioni di lavoro su piattaforma Windows che assumono la funzione di client rispetto ai servizi forniti dai sistemi presenti a livello centrale CED.

4.1.1. ARCHITETTURA A LIVELLO CENTRALE

Il Centro di Elaborazione Dati (CED) è il punto centrale di tutta l'infrastruttura di rete del Comune di Como.
I principali sistemi, localizzati presso il CED, sono i seguenti:

- centos ;
- debian ;
- fedora;
- red hat;
- ubuntu;
- vmware esxi 4.1;
- i sistemi Windows 2008 Server;

- i sistemi Windows 2003 Server;
- il sistema Windows 2000 server
- le periferiche di memorizzazione e di stampa;
- i server e dispositivi di rete;
- postazioni di lavoro per la gestione operativa dei dispositivi;

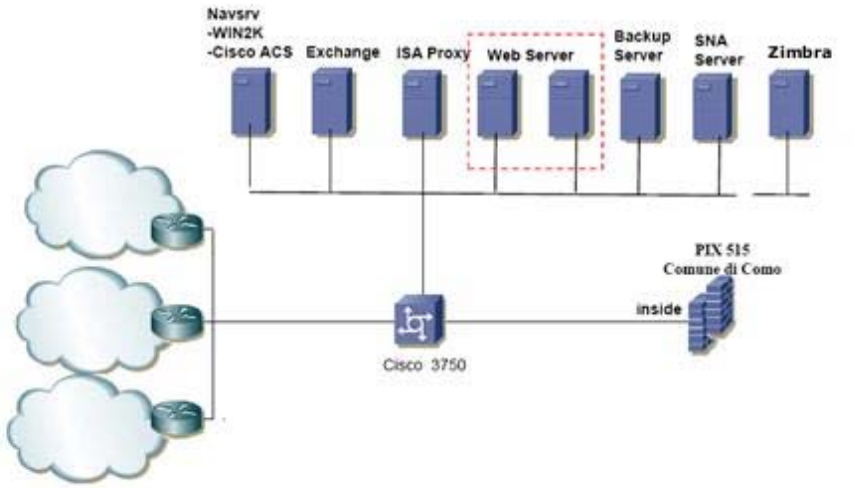


Figura 2 Architettura livello centrale

4.1.2 ARCHITETTURA UFFICI

Gli uffici sono composti generalmente da una LAN ethernet su cui si attestano delle workstation che operano come client. Non sono presenti apparati o sistemi complessi.

4.2 IDENTIFICAZIONE RISORSE DATI

I dati sono stati identificati e classificati secondo varie tipologie di dati suddivise in **dato personale, dato sensibile e dato giudiziario**.
Il trattamento di dati personali effettuato riguarda esclusivamente le seguenti informazioni:

- lavoratori dipendenti, anche se prestatori di lavoro temporaneo o in rapporto di tirocinio, apprendistato e formazione e lavoro ad associati anche in compartecipazione ed ai relativi familiari e conviventi;
- consulenti e liberi professionisti, agenti, rappresentanti e mandatari e soggetti che effettuano prestazioni coordinate e continuative;
- altri lavoratori autonomi in rapporto di collaborazione con i soggetti di cui al punto precedente;

- terzi danneggiati nell'esercizio dell'attività lavorativa o professionale dai soggetti di cui ai precedenti punti.
- utenti anche potenziali;
- fornitori di beni e servizi, agenti e rappresentanti;
- soggetti od organismi pubblici;
- visitatori occasionali;

Nella tabella che segue sono identificati gli archivi rilevati in seguito ad un'indagine condotta intervistando i responsabili delle aree e degli uffici.

Denominazione Archivio/banca dati	**Descrizione Archivio /Banca Dati**
DB Giuridica	Banca dati contiene informazioni giuridiche del personale. Sono trattati tutti gli aspetti giuridico e amministrativi del rapporto di lavoro con l'Ente, dalla primissima fase di ricognizione del fabbisogno a quella di reclutamento e selezione fino a terminare con quella di cessazione, contiene inoltre i fascicoli personali del dipendente e viene utilizzata per la raccolta e la trasmissione, previo controllo ed elaborazione, dei dati giuridici necessari per la formazione degli stipendi al Settore Ragioneria-Ufficio Stipendi e Pensioni. Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune.
DB Presenze	Banca dati contenente le informazioni relative alla rilevazione delle presenze personale dipendente. È utilizzata per la gestione del controllo delle presenze con riferimento sia alle ferie che alla gestione di malattie ed infortuni e del servizio della mensa per il personale dipendente; è predisposta inoltre al servizio degli obiettori di coscienza.
DB Stipendi	È utilizzata per la corresponsione del trattamento economico del personale dipendente di ruolo e a tempo determinato. Fornisce i dati sui quali effettuare il calcolo e il versamento dei contributi previdenziali obbligatori e delle ritenute fiscali, nonché degli oneri a carico dell'Ente. Permette di predisporre inoltre il conto annuale del personale, e di compilare le dichiarazioni CUD annuali, tratta le denunce d'infortunio e le certificazioni ai fini dell'indennità di disoccupazione.
DB Anagrafe DB Stato Civile DB Elettorale	È utilizzata dal Servizio Anagrafe che tiene il registro della popolazione residente a Como e dei cittadini trasferiti all'Estero ed opera in collaborazione con tutti gli Enti Pubblici ed Istituzionali per il rilascio d'ufficio dei certificati di: • Residenza, Cittadinanza, Stato di Famiglia, Godimento diritti politici, Stato libero, Esistenza in vita e Iscrizione alle liste elettorali; • Cambiamento di indirizzo • Trasferimento di residenza da altro Comune • Trasferimento di residenza all'Estero • Certificati anagrafici redatti a mano - Albero genealogico • Carta di identità • Certificato di identità per minori di anni 15 • Atto notorio: dichiarazione sostitutiva di atto notorio • Autenticazioni • Cambiamento della qualifica professionale (sulla carta di identità). • Gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE) • Attività di gestione dei registri di stato civile • Attività relativa alla tenuta dell'elenco dei giudici popolari • Attività relativa alla tenuta del registro degli obiettori di coscienza • Attività relativa alla tenuta delle liste di leva e dei registri matricolari

	Inoltre, l'accesso in sola visione a tali Data Base è necessario per il corretto svolgimento delle attività dei seguenti settori del Comune di Como: Archivio, Messi, Tributi, Polizia locale, Decentramento ,Circoscrizioni.
DB Risultati Elezioni	Banca Dati che contiene le informazioni inerenti ai risultati elettorali. • Attività relativa all'elettorato attivo e passivo
DB Albo Giudici Popolari	Banca Dati che contiene l'elenco dei giudici popolari .
DB Albo Presidenti di Seggio	Banca Dati che contiene l'albo dei presidenti di seggio . Attività relativa alla tenuta degli albi dei presidenti di seggio .
DB Albo Scrutatori	Banca Dati che contiene l'albo scrutatori. Attività relativa alla tenuta degli albi degli scrutatori .
DB Protocollo	Le funzionalità della banca dati sono legate alle attività connesse alla ricezione delle pratiche per via diretta o per posta, al protocollo, alla movimentazione e alla conservazione degli atti comunali e al loro riordino. Tutta la corrispondenza diretta all'Ente o in partenza dall'Ente medesimo passa infatti per l'ufficio Archivio e Protocollo per essere protocollata, registrata, classificata, inserita in fascicoli per argomenti, assegnata ai Settori per competenza.
DB ICI/IMU	La banca dati contiene tutte le informazioni necessarie per il calcolo, la riscossione e il controllo, dell'Imposta Comunale sugli Immobili (I.C.I.) e dell'Imposta Municpale Unica (IMU) che deve essere pagata da tutti coloro che possiedono fabbricati, aree fabbricabili e terreni agricoli come proprietari oppure come titolari di diritti reali di godimento.
DB Contabilità (finanziaria)	Banca dati necessaria per la tenuta della contabilità economica, finanziaria e patrimoniale di tutte le spese comunali e alla verifica sull'andamento delle stesse. Contiene dati relativi alla tenuta dei registri IVA. Utilizzata dall'ufficio Ragioneria per impegnare, liquidare, emettere mandati di pagamento in favore dei fornitori di beni e servizi, mediante la Tesoreria comunale.
DB Economato	Banca dati utilizzata dal Settore Economato per la fornitura di beni e servizi per i vari uffici e servizi comunali e per gestire: • tenuta e aggiornamento beni inventariati; • gestione cassa economale • gestione cassa contratti
DB Contravvenzioni	La banca dati è utilizzata per l'elaborazione amministrativa di tutte le contravvenzioni comminate dalla Sezione Operativa per infrazioni al Codice della Strada, ai regolamenti comunali e alle altre normative del Settore.
DB Tassa Rifiuti/TARES	La banca dati Tarsu /Tares è utilizzata dall'Ufficio tributi per la determinazione il calcolo e la riscossione della Tassa per lo smaltimento dei rifiuti solidi urbani.
DB Cosap	La banca dati Cosap Contiene le informazioni inerenti alle occupazioni di suolo pubblico appartenente al demanio o al patrimonio indisponibile del Comune e aree assimilate, nonché dello spazio ad esso sovrastante o sottostante, sono soggette a concessione oltre che al pagamento di un canone (Canone di Occupazione Spazi e Aree Pubbliche - C.O.S.A.P.).
DB Pubblicità	La banca dati (PUB) Pubblicità è utilizzata per la gestione delle entrate derivanti da pubblicità. Per semplicità sono state trattate in modo unificato.
DB U.T.E. Catasto	La banca dati che contiene le informazioni inerenti al catasto degli immobili e della conservatoria
DB Condono	La banca dati è utilizzata dal Settore Giuridico/ Amministrativo per gestire l'istruttoria delle pratiche di condono .
DB Lavori Pubblici	La banca dati è utilizzata dal Settore Lavori pubblici per provvedere alla predisposizione di tutti gli atti amministrativi, relativi all'esecuzione dei Lavori Pubblici, in conformità a progetti redatti dai vari Settori dell'Ufficio Tecnico Comunale.

DB Pratiche Edilizia Privata	La banca dati è utilizzata dal Settore Edilizia privata per gestire l'istruttoria delle pratiche edilizie rilasciando i provvedimenti che permettono l'esecuzione degli interventi edilizi.
DB Anagrafica Messi	Banca dati contenente le informazioni relative alle notifiche.
DB Biblioteca	Banca dati utilizzata per la gestione dell'iscrizione sia alla lettura in sede (libera a tutti) che per il prestito a domicilio (riservato ai residenti o domiciliati nelle Province di Como e Lecco e nel Canton Ticino) è necessario la presentazione di un documento di identità. Per i ragazzi fino ai 15 anni è richiesta la presenza di un genitore o sua delega scritta.
DB accessi internet Biblioteca	
DB Museo Civico	Banca dati contenente informazioni relative alle attività di studio nel museo civico.
DB Attività Produttive	La banca dati è utilizzata per la gestione dei procedimenti relativi ad atti e provvedimenti concernenti l'apertura, la modifica e la cessazione delle attività produttive, nonché per provvedimenti di polizia amministrativa.
DB Patrimonio Comunale	La banca dati è utilizzata per la gestione del patrimonio disponibile del Comune di Como ed è utilizzata per: • la gestione degli immobili compresi nel demanio comunale e nel patrimonio indisponibile temporaneamente sottratti all'uso da parte della generalità dei cittadini (beni monumentali dati in concessione, porzioni di edifici pubblici non utilizzate a fini istituzionali, parcheggi custoditi a pagamento ecc..); • le acquisizioni e le vendite di immobili in via bonaria, con esclusione di quelle di competenza del settore edilizia convenzionata e Sovvenzionata - aree PEEP, allargamenti stradali ecc.. - e delle acquisizioni effettuate con procedura espropriativa per pubblica utilità.
DB Istruzione	Banca dati utilizzata per gestire i servizi relativi al diritto allo studio; contiene dati relativi ai cittadini a cui vengono erogati servizi suddetti.
DB Anagrafica Servizi Sociali	Banca dati utilizzata per gestire le politiche sociali. Contiene dati relativi ai cittadini a cui vengono erogati servizi sociali. In particolare è utilizzata per erogare servizi che si esplicano nelle attività relative: • all'assistenza domiciliare • all'assistenza scolastica ai portatori di handicap o con disagio psico-sociale • alla richiesta di ricovero in Istituti, Case di cura, Case di riposo; • alle attività ricreative per la promozione del benessere della persona e della comunità, per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale • alla valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionali o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagio psico-sociali) • all'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro diurno, centro socio educativo, ludoteca, ecc.) • al sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico trasporto • alla prevenzione ed al sostegno alle persone tossicodipendenti ed alle loro famiglie tramite centri di ascolto (per sostegno) e centri documentali (per prevenzione) • ai sevizi di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori • ai trattamenti sanitari obbligatori (T.S.O.) ed all'assistenza sanitaria obbligatoria (A.S.O.) • alla concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica
DB Avvocatura	• Banca dati utilizzata per gestire le attività relative alla consulenza giuridica, nonché al patrocinio ed alla difesa in giudizio dell'amministrazione.

DB sinistri e assicurazioni	Banca dati relativa all'apertura di sinistri ed al riconoscimento degli indennizzi
DB Polizia locale	Banca dati contente tutti le informazioni necessarie al corretto svolgimento delle attività: • relative all'infortunistica stradale • di polizia annonaria, commerciale e amministrativa • di vigilanza edilizia, in materia di ambiente e sanità nonché di polizia mortuaria • relative al rilascio di permessi per invalidi
DB Servizi Cimiteriali	Banca dati contente i dati e le informazioni per individuare la collocazione delle tombe nei 9 cimiteri della città.
DB SVP (Valutazione del Personale)	Banca dati contente tutte le informazioni relative alla valutazione sull'operato dei dipendenti comunali.
DB Progressioni	Banca dati contente tutte le informazioni relative alle progressioni orizzontali dei dipendenti comunali.
DB PEG	Banca dati contente tutte le informazioni relative al piano esecutivo di gestione.
DB Merloni	Banca dati contente tutti le informazioni relative al calcolo dell'incentivo spettante dalla legge Merloni.
DB Contratti	Banca Dati contenente tutti i dati relativi ai contratti stipulati dall'Ente in seguito a gare d'appalto ad evidenza pubblica ed ai contratti di locazione, di concessione di beni immobili di proprietà comunale
DB Vigile Elettronico	Banca dati contente tutti le informazioni necessarie al corretto svolgimento delle attività: • relative al rilascio permessi ZTL • relative al rilascio di permessi per invalidi • rilevazione accessi dei veicoli nel centro storico Il sistema è stato autorizzato dal Ministero dei Trasporti e garantisce la sicurezza dei dati raccolti come previsto dalla normativa sulla privacy. La responsabilità di tutte le operazioni connesse al controllo e all'eventuale contravvenzione è della Polizia locale.
DB Ufficio relazioni con il pubblico	Banca Dati contenente i dati relativi ai seguenti servizi: • rinvenimento oggetti smarriti • segnalazioni e reclami • indagini di customer satisfaction • registrazione propedeutica per l'utilizzo di servizi avanzati del portale (livello 3) • portale vocale
DB Ufficio stampa	Banca dati contenente dati necessari per l'invio di informazioni mediante: sms, newsletter informative, periodico "Il cittadino" e media list
DB Segreteria	Banca dati utilizzata per la gestione delle determinazioni dirigenziali, delle delibere di giunta e di consiglio comunale
DB Politiche giovanili	Banca dati contenente le informazioni necessarie per il rilascio della Card giovani e per l'invio di una newsletter giovani

Tabella 1 Descrizione archivi

Nella tabella seguente per ogni banca dati identificata si riportano le informazioni sotto elencate:

1. **Denominazione Archivio/banca dati:** Sigla identificativa della Banca dati individuata nella fase di rilevazione;
2. **Dati :** tipologia dei dati trattati, (personale, sensibile);
3. **Trattamento elettronico:** indica se la modalità di trattamento è mediante l'ausilio di strumenti elettronici;
4. **Supporto cartaceo:** indica se il supporto di memorizzazione dei dati trattati è cartaceo, inoltre si indica dove/come sono custoditi i documenti.

Denominazione Archivio / banca dati	Dati	Trattamento elettronico	Supporto cartaceo
DB Giuridica	P/S	Si	Schedario in Armadio
DB Presenze	P	Si	Schedario in Armadio
DB Stipendi	P/S	Si	Schedario in Armadio
DB_Anagrafe DB_Elettorale DB_Risultati Elezioni DB_Stato Civile DB_Albo_Scrutatori DB_Albo_Presidenti di Seggio DB_Albo_Giudici _Popolari	P P P P/S P/S P/S P/S	Si	Schedario in armadi ignifughi con chiusura semi automatizzata
DB Protocollo	P	Si	Schedario in Armadio
DB U.T.E. Catasto	P	Si	Schedario in Armadio
DB Condono	P/S	Si	Schedario in Armadio
DB ICI/IMU	P	Si	Schedario in Armadio
DB Contabilità	P	Si	Schedario in Armadio
DB Economato	P	Si	Schedario in Armadio
DB Contravvenzioni	P/S	Si	Schedario in Armadio
DB Tarsu	P	Si	Schedario in Armadio
DB Cosap	P	Si	Schedario in Armadio
DB Pubblicità	P	Si	Schedario in Armadio
DB Lavori_Pubblici	P	Si	Schedario in Armadio
DB Pratiche Edilizia Privata	P	Si	Schedario in Armadio
DB Anagrafica Messi	P	Si	Schedario in Armadio
DB Biblioteca	P/S	Si	Schedario in Armadio
DB accessi internet Biblioteca	P/S	No	Schedario in Armadio
DB Museo Civico	P	Si	Schedario in Armadio
DB Attività Produttive	P/S	Si	Schedario in Armadio
DB Patrimonio Comunale	P	Si	Schedario in Armadio
DB Servizi Cimiteriali	P/S	Si	Schedario in Armadio
DB SVP	P/S	Si	Schedario in Armadio
DB PEG	P/S	Si	Schedario in Armadio
DB Progressioni	P/S	Si	Schedario in Armadio
DB Merloni	P/S	Si	Schedario in Armadio
DB Istruzione	P/S	Si	Schedario in Armadio
DB Anagrafica Servizi Sociali	P/S	Si	Schedario in Armadio
DB Contratti	P/S	Si	Schedario in Armadio
DB Avvocatura	P/S/G	Si	Schedario in Armadio
DB Sinistri e assicurazioni	P/S	Si	Schedario in Armadio
DB Polizia locale	P/S/G	Si	Schedario in Armadio
DB Vigile elettronico	P/S	Si	Schedario in Armadio
DB Urp	P/S	Si	Schedario in Armadio
DB Ufficio Stampa	P/S	Si	Schedario in Armadio

DB Politiche giovanili	P/S	Si	Schedario in Armadio
DB Segreteria	P/S	Si	Schedario in Armadio

Tabella 2 Identificazione archivi e banche dati

4.3 PROCEDURE INFORMATIZZATE

Sono state individuate nell'architettura applicativa dell'Ente, le seguenti procedure informatizzate utilizzate per il trattamento dei dati personali. Per ogni procedura sono stati individuati gli utilizzatori e le Basi dati.

Procedure informatizzate	**Utilizzatori**	**Base dati**
Gestione giuridica personale	Risorse umane	DB_ Giuridica
Gestione presenze	Risorse umane	DB_ Presenze
Gestione stipendi	Servizi Finanziari	DB_ Stipendi
Sistema demografico: • Anagrafe elettorale • Gestione risultati elettorali • Albo scrutatori • Stato civile	Con funzionalità complete • Servizi demografici In consultazione: • Questura • Comando Provinciale Carabinieri • Circoscrizioni • Polizia stradale • Creset • OSA	DB_Anagrafe DB_Elettorale DB_ Risultati Elezioni DB_ Stato_Civile DB_ Albo_Scrutatori DB_Albo_Presidenti di seggio DB_Giudici Popolari
Protocollo e archivio	Archivio	DB_ Protocollo
Tributi_ICI	Servizi Finanziari	DB_ICI
Sistema contabilità finanziaria	Servizi Finanziari	DB_ Contabilità
Sistema gestione economato Magazzino	Provveditorato	DB_ Economato
Sistema gestione contravvenzioni	Polizia locale	DB_ Contravvenzioni
Tarsu – Pubblicità – Cosap	Servizi Finanziari	DB_ Tarsu DB_ Cosap DB_Pubblicità
Gestione progettazione dei lavori	Lavori pubblici	DB_ Lavori Pubblici DB_U.T.E. Catasto
Sistema gestione pratiche edilizia privata	Edilizia privata	DB Pratiche Edilizia Privata
Sistema Gestionale pratiche condono	Settore Giuridico/Amministrativo	DB_Condono
Gestione messi comunali	Messi Comunali	DB Anagrafica Messi Comunali
Biblioteca: inventariazione, gestione prestito e gestione del soggetta rio	Biblioteca Amministrazione Prov.le - Cultura	DB_ Biblioteca DB accessi internet Biblioteca
Biblioteca Museo Civico: Inventariazione	Museo Civico	DB_ Museo Civico
Attività produttive e polizia amministrativa	Settore Attività Produttive	DB_Attività_Produttive
Gestione patrimonio comunale	Patrimonio	DB_ Patrimonio
Gestione Istruzione	Istruzione	DB_Istruzione
Gestione Servizi_Sociali	Servizi Sociali	DB_Anagrafica Servizi Sociali
Avvocatura	Contenzioso e sinistri	DB_Avvocatura
Gestione assicurazioni	Contenzioso e sinistri	DB_Sinistri e assicurazioni

Gestione Servizi Polizia Locale	Polizia Locale	DB_ Polizia locale
Gestione Vigile Elettronico	Polizia Locale	DB_Vigile_Elettronico
Gestione Servizi Cimiteriali	Provveditorato	DB_Servizi_Cimiteriali
Gestione contratti	Contratti e uff. gare	DB_Contratti
Sistema di Valutazione del Personale	Controllo di Gestione	DB_SVP
Gestione delle progressioni orizzontali	Controllo di Gestione	DB_PROGRESSIONI
Gestione PEG	Controllo di Gestione	DB_WEBPEG
Software Merloni	Settore Tecnico – OO. PP.	DB_MERLONI
Gestione software per: rinvenimento oggetti smarriti, segnalazioni e reclami, indagini di customer satisfaction, registrazione propedeutica per l'utilizzo di servizi avanzati del portale (livello 3), portale vocale	Uff. stampa, Urp, Comunicazione	DB URP
Gestione software per invio sms, newsletter informative, periodico "Il cittadino" e media list	Uff. stampa, Urp, Comunicazione	DB Ufficio stampa
Gestione software per rilascio della Card giovani e per l'invio di una newsletter giovani	Politiche giovanili	DB Politiche giovanili
Gestione delle determinazioni dirigenziali, delle delibere di giunta e di consiglio comunale.	Segreteria Generale	DB Segreteria

Tabella 3 Procedure informatizzate

5. ELENCO DEI TRATTAMENTI

Il trattamento dei dati indicati nel paragrafo precedente è necessario per i seguenti scopi:

- **adempiere o esigere l'adempimento di specifici obblighi** o eseguire specifici compiti previsti da leggi, dalla normativa comunitaria da regolamenti o da contratti collettivi, in particolare ai fini del rispetto della normativa in materia di previdenza ed assistenza anche integrativa, o in materia di igiene e sicurezza del lavoro o della popolazione, nonché in materia fiscale, di tutela della salute, dell'ordine e della sicurezza pubblica;
- **in conformità alla legge** e per scopi determinati e legittimi, ai fini della tenuta della contabilità o della corresponsione di stipendi, assegni, premi, altri emolumenti, liberalità o benefici accessori;
- **far valere o difendere un diritto** anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi. Nel caso in cui i dati siano idonei a rivelare lo stato di salute e la vita sessuale, il diritto da far valere o difendere deve essere di rango pari a quello dell'interessato.
- **l'esercizio del diritto di accesso** ai documenti amministrativi, nel rispetto di quanto stabilito dalle leggi e dai regolamenti in materia.
- **adempiere ad obblighi derivanti da contratti** di assicurazione finalizzati alla copertura dei rischi connessi alla responsabilità del datore di lavoro in materia di igiene e di sicurezza del lavoro e di malattie professionali o per i danni cagionati a terzi nell'esercizio dell'attività lavorativa o professionale.
- **garantire le pari opportunità.**

Per adempiere ad alcune delle finalità suddette i dati trattati sono comunicati anche per via telematica ad organi, enti o società preposti.

5.1.1. TRATTAMENTO DATI SENSIBILI

I Comuni che hanno iniziato a trattare dati di carattere sensibile o giudiziario anteriormente al 1 gennaio 2004, qualora si rinvenga nell'ordinamento una disposizione di legge che specifichi unicamente le finalità di rilevante interesse pubblico ma non la tipologia di dati trattabili e di operazioni eseguibili, sono tenuti ad identificare e rendere pubblici i tipi di dati e di operazioni realizzabili attraverso un atto di natura regolamentare**,** adottato in conformità al parere espresso dal Garante anche su schemi tipo (artt. 20, comma 2, e 181, comma 1, lett. a), del d.lg. n. 196/2003). Il Comune di Como ha partecipato alla fase di consultazione su internet del suddetto regolamento, in collaborazione con il "garante della privacy". Il regolamento è stato approvato con delibera del Consiglio Comunale n. 25 del 20.3.2006. Nella tabella seguente si evidenziano le tipologie di trattamento di dati sensibili identificate. Ad ogni trattamento è associato il settore o il servizio autorizzato a tale trattamento.

Settore/Servizio	Denominazione del trattamento
Personale/Risorse Umane	Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune
	Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il comune - attività relativa al riconoscimento di benefici connessi all'invalidità civile per il personale.
Servizi demografici/Anagrafe	Gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)
Servizi demografici/Stato Civile	Gestione e aggiornamento dei registri di stato civile
Servizi demografici/Elettorale	Gestione e aggiornamento relativo all'elettorato attivo e passivo
	Aggiornamento degli albi degli scrutatori e dei presidenti di seggio
	Aggiornamento dell'elenco dei giudici popolari
Servizi sociali	Attività relativa all'assistenza domiciliare
	Attività relativa all'assistenza scolastica ai portatori di handicap o con disagio psico-sociale
	Attività relativa alla richiesta di ricovero in Istituti, Case di cura, Case di riposo, ecc.
	Attività ricreative per la promozione del benessere della persona e della comunità, per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale
	Attività relativa alla valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionali o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagio psico-sociale)
	Attività relativa all'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro diurno, centro socio educativo, ludoteca, ecc.)
	Attività di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico trasporto
	Attività relativa alla prevenzione ed al sostegno alle persone tossicodipendenti ed alle loro famiglie tramite centri di ascolto (per sostegno) e centri documentali (per prevenzione)
	Attività relativa ai sevizi di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori

	Attività relativa ai trattamenti sanitari obbligatori (T.S.O.) ed all'assistenza sanitaria obbligatoria (A.S.O.)
	Attività relativa alla concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica
Istruzione e cultura	Attività relativa alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne
	Attività di formazione ed in favore del diritto allo studio
	Gestione delle biblioteche e dei centri di documentazione e dei servizi di accesso all'internet point
Polizia locale	Attività relativa all'infortunistica stradale
	Gestione delle procedure sanzionatorie
	Attività di polizia annonaria, commerciale e amministrativa
	Attività di vigilanza edilizia, in materia di ambiente e sanità nonché di polizia mortuaria
	Attività relativa al rilascio di permessi per invalidi
Avvocatura e sinistri	Attività relativa alla consulenza giuridica, nonché al patrocinio ed alla difesa in giudizio dell'amministrazione e alla gestione dei sinistri e relative richieste di rimborso
Contratti – uff. gare	Attività relativa alla stipula di contratti di locazione di beni immobili di proprietà comunale (in particolare alloggi popolari) e di redazione di contratti di lavori pubblici in seguito a gara ad evidenza pubblica
Attività Produttive	Attività relativa al rilascio, alla modifica e alla revoca di provvedimenti amministrativi in materia di attività produttive e di polizia amministrativa
Politiche del lavoro	Gestione delle attività relative all'incontro domanda/offerta di lavoro, comprese quelle relative alla formazione
Servizi demografici/Leva	Attività relativa alla tenuta delle liste di leva e dei registri matricolari
Urp	Gestione delle informazioni fornite e delle segnalazioni ricevute, dei reclami, del rinvenimento di oggetti smarriti

Tabella 4 Trattamenti sensibili

6. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ

6.1 TITOLARE DEL TRATTAMENTO

Ai sensi dell'art. 4 del Codice, il titolare del trattamento dei dati personali è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
Con delibera di Giunta n. 308 del 9.11.2005, Titolare del trattamento dei dati personali è il Comune di Como con sede in Como, via Vittorio Emanuele II n. 97, nella persona del Sindaco pro tempore.
Il Titolare del trattamento dei dati personali nomina i Responsabili nei termini richiesti dall'art. 29 del Codice.

6.2 RESPONSABILE DEL TRATTAMENTO

E' designato Responsabile la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

Per effetto dell'articolo 29 del Codice il responsabile è designato dal titolare ed è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
Per esigenze organizzative, possono essere designati responsabili più soggetti, mediante suddivisione di compiti analiticamente specificati per iscritto dal titolare.
Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle proprie istruzioni.
Nell'ambito del Comune di Como, con nota del Sindaco, sono state nominate le figure di "Responsabile del Trattamento dei dati personali", ognuna relativamente alla banca dati che gestisce.
L'elenco aggiornato dei Responsabili del trattamento dei dati personali dell'Ente è consultabile presso l'ufficio Personale del Comune di Como.
Inoltre:

- al Responsabile dei Sistemi Informativi è attribuita anche una responsabilità specifica relativamente alla sicurezza di tutti i dati personali trattati con l'ausilio di strumenti elettronici utilizzati dal Comune di Como;
- le Società che svolgono servizi in outsourcing per l'Ente e che in tale ambito trattano dati personali dell'Ente, sono nominate Responsabili del trattamento dei dati necessari per l'espletamento delle attività connesse al servizio richiesto.

6.3 INCARICATO DEL TRATTAMENTO

Ai sensi dell'art. 30 del Codice sono Incaricati del trattamento dei dati personali le persone fisiche autorizzate a compiere operazioni di trattamento dal Responsabile. L'incaricato, nell'adempiere le proprie mansioni di trattamento dei dati, si attiene scrupolosamente alle direttive ricevute dal Responsabile. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad un'unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima. Agli incaricati sono attribuiti livelli di accesso differenziati sulla base del ruolo professionale ricoperto. Tale differenziazione degli accessi è garantita dal sistema di riconoscimento delle credenziali di identificazione e autenticazione e del profilo utente in uso.
Nella lettera di incarico il Responsabile impartisce le istruzioni necessarie a garantire la segretezza della componente riservata delle credenziali di autenticazione. L'Amministrazione archivia nella cartella personale del dipendente la copia della lettera di nomina a Responsabile e ad Incaricato del trattamento e comunica al Centro elaborazione dati le cessazioni, affinché si provveda – tramite l'amministratore di sistema - alla disattivazione di tutte le utenze assegnate al cessato.

6.4 AMMINISTRATORI DI SISTEMA

Con atto sindacale del 26 giugno, prot. 30022 del 29.6.2009, il Titolare del trattamento ha nominato amministratore di sistema il sig. Salvatore Di Martino. Successivamente, in data 15.12.2009 è stato individuato quale ulteriore amministratore di sistema il Sig. Marco Gabaglio. Alle figure sopracitate, che sono state individuate previa valutazione delle caratteristiche di esperienza, capacità e affidabilità, in quanto forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza, è stato assegnato il compito di sovrintendere alle risorse del sistema informativo del Comune:

- Individuando, con atto scritto il/i soggetto/i incaricato/i della custodia delle parole chiave per l'accesso al sistema informativo e vigilando sulla sua attività;
- impostando e gestendo un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dai punti da 1 a 10 del Disciplinare tecnico, allegato B) al D. Lgs. n. 196/2003;
- impostando e gestendo un sistema di autorizzazione per gli incaricati dei trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dai punti da 12 a 14 del Disciplinare tecnico, allegato B) al D. Lgs. n. 196/2003;
- verificando che il Comune abbia adottato le misure minime di sicurezza per il trattamento dei dati personali, previste dagli art. dal 31 al 34 del D. Lgs. n. 196/2003, e dal Disciplinare tecnico, allegato B) al decreto legislativo medesimo, provvedendo agli adeguamenti eventualmente necessari;
- suggerendo l'adozione e l'aggiornamento delle più ampie misure di sicurezza atte a realizzare quanto previsto dall'art. 31 del D. Lgs. n. 196/2003, che dispone che i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da 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;
- curando l'adozione e l'aggiornamento delle eventuali misure "idonee" di cui al punto precedente;
- attivando e aggiornando con cadenza almeno semestrale idonei strumenti elettronici atti a proteggere i dati trattati attraverso gli elaboratori del sistema informativo contro il rischio di intrusione e contro l'azione dei virus informatici;
- aggiornando periodicamente, con frequenza almeno annuale (*oppure* semestrale *se si trattano dati sensibili o giudiziari*), i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti;
- impartendo a tutti gli "operatori di sistema" istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale;
- adottando procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
- predisponendo un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, dell'efficacia delle misure di sicurezza adottate in azienda.
- riferendo periodicamente, ed in ogni caso con cadenza annuale, al Titolare sullo svolgimento dei Suoi compiti, dandogli inoltre piena collaborazione nello svolgimento delle verifiche periodiche circa il rispetto delle disposizioni di legge e l'adeguatezza delle misure di sicurezza adottate.

All'amministratore di sistema, relativamente alle applicazioni in uso, compete altresì il compito di:

- sovrintendere alle risorse del sistema operativo e/o del sistema di base dati e di consentirne l'utilizzazione per la sede di competenza;
- assegnare/revocare al personale abilitato, su indicazione del rispettivo Responsabile, le autorizzazioni all'utilizzo di specifiche procedure applicative, evidenziando la delimitazione degli ambiti di accesso alle suddette procedure;
- attribuire/comunicare al personale abilitato la password iniziale, e la chiave di accesso personale per l'utilizzazione dell'elaboratore e fornire ogni istruzione in merito alle appropriate modalità di selezione e custodia della chiave di accesso personale e della password;
- conservare, aggiornare e verificare l'elenco degli amministratori, al fine di assicurare la sospensione delle chiavi di accesso in caso di revoca dell'incarico o di mancato utilizzo della stessa chiave;

- proteggere il sistema informatico ad essi affidato dal rischio di intrusione.

In questo paragrafo si fornisce una mappa in formato tabellare che associa ad ogni Banca Dati precedentemente individuata le relative responsabilità. I responsabili procedono alla nomina dei "preposti alla custodia della parola chiave" cui è affidato il compito di conservare in luogo non accessibile (armadio/cassettiera chiusa a chiave) le buste chiuse contenenti le parole chiave degli incaricati, il cui contenuto deve restare segreto. Ogni busta custodita potrà essere consegnata al lavoratore che l'ha depositata o al Responsabile del trattamento dati o persona delegata.

Archivio/banca dati	Settori incaricati del trattamento	Responsabile - Dirigente
DB_ Presenze DB_ Giuridica DB_ Progressioni DB_ Sistema Valutazioni Personale	Settore Risorse Umane	Dott. Raffaele Buononato
DB_ Stipendi	Settore Servizi Finanziari, Entrate Tributarie	Dott. Raffaele Buononato
DB_Anagrafe DB_Elettorale DB_Risultati Elezioni DB_Stato Civile DB_Albo_Scrutatori DB_Albo_Presidenti di Seggio DB_Albo_Giudici Popolari	Servizi Demografici In sola visione: Questura	Dott.ssa Domizia De Rocchi
DB_ Protocollo	Archivio, Protocollo, Decentramento	Dott. Massimo Patrignani
DB_ ICI/IMU	Settore Servizi Finanziari, Entrate Tributarie	Dott. Raffaele Buononato
DB_ Contabilità	Settore Servizi Finanziari, Entrate Tributarie	Dott. Raffaele Buononato
DB_ Economato	Settore Provveditorato	Dott. Raffaele Buononato
DB_ Contravvenzioni	Settore Polizia Locale e Sicurezza	Dott. Vincenzo Graziani
DB_ Tarsu/TARES	Settore Servizi Finanziari, Entrate Tributarie	Dott. Raffaele Buononato
DB_ Cosap	Settore Servizi Finanziari, Entrate Tributarie	Dott. Raffaele Buononato
DB_ Pubblicità	Settore Servizi Finanziari, Entrate Tributarie	Dott. Raffaele Buononato
DB_ Lavori_Pubblici DB_U.T.E. Catasto	Settore Edilizia Pubblica	Ing. Antonio Ferro
DB_Pratiche_Edilizia_Privata	Settore Pianificazione Urbanistica – Edilizia Privata	Ing. Giuseppe Cosenza
DB_Condono	Settore Giuridico/Amministrativo	Dott.ssa Rossana Tosetti
DB_Anagrafica Messi	Segreteria Generale	Avv. Marina Ceresa
DB_ Biblioteca	Settore Cultura - Musei - Biblioteca	Dott. Maurizio Ghioldi
DB_ accessi internet Biblioteca	Settore Cultura - Musei - Biblioteca	Dott. Maurizio Ghioldi
DB_ Museo_Civico	Settore Cultura - Musei - Biblioteca	Dott. Maurizio Ghioldi
DB_Attività_Produttive	Settore Attività Produttive	Dott. Massimo Patrignani
DB_ Patrimonio_Comunale	Settore Patrimonio	Dott.ssa Rossana Tosetti
DB_Istruzione	Settore Politiche educative	Dott.ssa Franca Gualdoni
DB_Anagrafica_Servizi_Sociali	Settore Servizi Sociali	Dott.ssa Franca Gualdoni

DB_Avvocatura DB Sinistri e assicurazioni	Settore Contenzioso e sinistri	Avv. Antonietta Marciano
DB_Polizia_locale DB_Vigile_elettronico	Settore Polizia Locale e Sicurezza	Dott. Vincenzo Graziani
DB_Contratti	Settore Contratti e uff. gare	Avv. Antonietta Marciano
DB Urp DB Ufficio stampa	Ufficio Stampa, Comunicazione, Urp	Dott. Maurizio Ghioldi
DB Segreteria Generale	Settore Segreteria Generale	Avv. Marina Ceresa

Tabella 5 Distribuzione delle responsabilità

7. ANALISI DEL RISCHIO

Il presente capitolo illustra i risultati dell'attività di gestione del rischio relativo al trattamento dei dati personali sensibili effettuata in passato dal comune di Como.. Nei paragrafi seguenti sono descritte:

- la metodologia adottata per effettuare l'Analisi dei Rischi con il prodotto CRAMM;
- il riassunto delle contromisure da implementare al fine di contrastare i rischi rilevati (gestione dei rischi) sulla base dei valori ottenuti dalla compilazione dei questionari di fase 1 (data asset) e di fase 2 (minacce e vulnerabilità).

Le contromisure proposte in questo documento sono relative a tutti gli asset individuati nel corso dell'attività di analisi del rischio del Sistema Informativo del Comune di Como.
L'analisi del rischio, è stata condotta con il supporto della metodologia CRAMM. Di seguito vengono descritte le linee guida di tale metodologia.

7.1 DESCRIZIONE DELLA METODOLOGIA ADOTTATA

7.1.1. LA METODOLOGIA CRAMM

Le caratteristiche più significative della metodologia CRAMM (CCTA Risk Analysis and Management Method) sono le seguenti:

- *Standard* - aderenza ai principali standard di sicurezza europei (BSI, ITSEC, …);
- *Consistenza* - sistemi simili con profili di rischio simili presentano soluzioni di sicurezza simili;
- *Flessibilità* - rapidi percorsi di revisione dell'analisi e rilevazioni più dettagliate;
- *Rigore* minacce e vulnerabilità ben identificate, rischi totalmente valutati e uso di misure rilevanti;
- *Auditability* - possibilità di verifica della corretta applicazione del metodo e dell'identificazione delle misure di sicurezza opportune.

CRAMM è la metodologia adottata dalla maggior parte dei dipartimenti governativi del Regno Unito e dagli enti governativi australiani; in Italia è la metodologia di analisi del rischio consigliata dal CNIPA.

7.1.2. LA GESTIONE DEI RISCHI

L'attività di gestione dei rischi è stata preceduta dall'analisi del rischio nel corso della quale sono stati valutati mediante interviste e/o questionari i seguenti aspetti:

- gli impatti sui dati che contribuiscono a determinare il Sistema Informativo ENTE;
- i livelli di vulnerabilità e minaccia che gravano su ciascun asset identificato al fine di determinare i rischi legati ai sistemi e alla rete.

La fase successiva, oggetto del presente capitolo, consiste nella gestione di tali rischi. L'obiettivo principale di questa fase è, quindi, l'identificazione del corretto insieme di contromisure che abbattano i rischi derivanti dalle minacce identificate nella fase precedente. Tali contromisure sono state selezionate sulla base dei valori della misura del rischio calcolata in precedenza.
Ogni singola fase che caratterizza l'attività di analisi del rischio con l'ausilio di CRAMM è stata documentata. La documentazione è fornita come allegato al presente documento ed è stata il punto di partenza per la stesura dei prossimi paragrafi.

7.2 APPLICAZIONE DELLE MISURE MINIME DI SICUREZZA

Le misure di sicurezza definiscono le regole, i criteri e la modalità che consentano di raggiungere gli obiettivi di sicurezza in funzione dei requisiti di disponibilità, integrità e riservatezza. L'applicazione di tali misure prende spunto dai risultati emersi dall'analisi del rischio.
Nel presente paragrafo sono analizzate ed indicate le modalità di implementazione delle misure minime di sicurezza, prescritte negli artt. 34,35 e 36 del Codice e descritte nell'allegato B dello stesso.

7.2.1. SISTEMA DI AUTENTICAZIONE INFORMATICA

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
Per l'accesso alle funzioni che interfacciano i dati personali registrati nei sistemi di elaborazione è prevista l'inserimento di identificativo dell'utente (chiave) e password:

- lunghezza della password non inferiore ad 8 caratteri
- scadenza automatica della password di rete ogni tre mesi
- per le applicazioni che non prevedono la possibilità di attuare un cambio password automatico gli utenti sono stati sensibilizzati a cambiarla frequentemente ed almeno una volta ogni tre mesi.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

- Le credenziali di autenticazione sono la combinazione di chiave e password.

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

- Ogni incaricato avendo la possibilità di accedere a funzioni diverse, ma comunque sempre vincolate dalle sue mansioni, dispone di più credenziali di autenticazione.

4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

- Si è sensibilizzato il personale a non diffondere le proprie credenziali di autenticazione ed a custodire in modo idoneo le parole chiave.

5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

- Le chiavi e le password di accesso ai PC e da questi verso la rete, sono generate e assegnate dal Centro di Elaborazione Dati; ogni utente modifica la propria password al primo accesso, e ogni tre mesi il sistema lo obbliga a rinominarla. Le attuali misure adottate sulla composizione delle password stabiliscono che la chiave non possa essere inferiore a 8 caratteri.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

- Il codice è personale e associato al dipendente, quindi univoco e non riutilizzabile.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

- Le credenziali di autenticazione di accesso alla rete e alle applicazioni per l'accesso ai dati sono disattivate se non utilizzate.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

- *L*a gestione dei dipendenti, prevede che in caso di dimissioni od allontanamento di un dipendente le sue credenziali siano disattivate.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

- Gli incaricati del trattamento di dati personali sono stati sensibilizzati in materia tramite circolari interne.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle

credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

- Non esistendo dati trattati esclusivamente da una sola persona, la situazione ipotizzata non si realizza, nel caso di assenza dell'incaricato. È responsabilità di ogni singolo settore assicurare la disponibilità dei dati o degli strumenti elettronici che esso utilizza.
- Il personale che ha il compito di gestire i sistemi di assegnazione delle credenziali di autenticazione e i responsabili dei settori precedentemente identificati sono stati nominati "custodi delle parole chiave".

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

- I dati personali destinati alla diffusione sono trattati a norma di legge.

7.2.2. SISTEMA DI AUTORIZZAZIONE

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

- I sistemi sono configurati per avere profili di autorizzazione in funzione dei ruoli rivestiti dagli incaricati.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

I ruoli sono assegnati anteriormente all'inizio del trattamento e sono determinati :

- automaticamente in base all'assegnazione del personale ai gruppi di lavoro predeterminati nell'ambito dell'organizzazione Comunale;
- definiti in funzione di specifiche richieste rivolte agli amministratori di sistema e convalidate dal Centro Elaborazione Dati.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

- Nell'ambito dei singoli settori la verifica sulla consistenza delle condizioni per la conservazione dei profili di autorizzazione è continua e posta in essere dal personale del Centro Elaborazione Dati.

7.2.3. ALTRE MISURE DI SICUREZZA

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla

manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

- L'elenco aggiornato degli incaricati e delle altre figure professionali previste dal Codice è tenuto presso l'ufficio personale, che ne verifica almeno annualmente la congruenza.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

- Su tutti i sistemi che lo consentono sono attivati programmi antivirus ed antintrusione aggiornati automaticamente in rete all'accensione.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

- L'aggiornamento è effettuato dal client Symantec (antivirus) presente su ogni PC ad ogni accesso al rete dell'Ente.
- Il client si collega direttamente con il Server Symantec e scarica automaticamente gli aggiornanti relativi ai nuovi virus.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

- Il salvataggio dei dati residenti sui sistemi presenti nel Centro elaborazione dati è almeno giornaliero. Responsabile del ripristino dei dati presenti nel CED è il centro di elaborazione dati.

7.2.4. ULTERIORI MISURE IN CASO DI TRATTAMENTO DI DATI SENSIBILI O GIUDIZIARI

19. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

- I dati sensibili e giudiziari, sono protetti mediante ulteriore barriera di autenticazione, sempre con chiave e password individuale.
- La gestione del sistema di autenticazione relativo alla gestione "stipendi" affidato a personale interno autorizzato.

20. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

- Il Settore Risorse Umane prevede nell'ambito del piano di formazione annuale incontri per l'aggiornamento

21. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

- I supporti sono sovrascritti.

22. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

- Presso il Centro Elaborazione Dati i supporti di salvataggio sono utilizzati sui sistemi di back-up per il ripristino delle funzionalità.
- Sono predisposte specifiche procedure di salvataggio e ripristino dei dati contenuti in archivi fisicamente non localizzati presso il CED.

7.2.5. MISURE DI TUTELA E GARANZIA

23. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

- L'eventuale trattamento da parte di soggetti esterni è garantito conforme al Codice in base a specifiche norme contrattuali.

24. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

- il presente documento è fatto proprio mediante una delibera di giunta comunale

25. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

- Sono impartite istruzioni scritte finalizzate al controllo ed alla custodia per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

7.2.6 TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

26. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate

- La documentazione cartacea relativa a dati personali sensibili o giudiziari è custodita in specifici locali ad accesso controllato entro i quali ne è possibile la visione.
- Non è consentito l'asporto di documentazione contenente dati personali sensibili o giudiziari.

27. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non

sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

- Gli archivi sono dotati procedure per l'accesso controllato e strumenti idonee per il controllo degli accessi.

8. INFORMAZIONI INTEGRATIVE

8.1. ULTERIORI MISURE DI SICUREZZA

A fronte del continuo evolversi delle tecnologie e della comparsa di nuove minacce, per conservare un livello idoneo di sicurezza vengono definite le seguenti le misure di sicurezza di supporto e miglioramento a quelle esistenti.

Misure relative agli incaricati:

- Vengono definite scadenze precise e più specifiche oltre le quali il dato deve essere eliminato da tutti i supporti che lo contengono.
- Il personale incaricato è istruito sul trattamento dei dati personali, con particolare attenzione verso quelli "sensibili", ed aggiornato periodicamente su quanto stabilito dalle leggi sulla Privacy.

Misure relative ai canali di trasmissione per i dati cartacei

- Per la tutela della "disponibilità" dei dati cartacei è opportuno che questi siano sempre sotto il controllo del personale adibito al loro trattamento, e che quindi non siano mai lasciati incustoditi.
- E' proibito lasciare a vista su scrivanie, fotocopiatrici, fax o altre postazioni, i documenti contenenti i dati trattati.

Misure relative ai locali nei quali sono riposti gli armadi contenitori

- E' predisposto un registro in cui annotare quali dati sono stati temporaneamente presi in carico e da chi.

Misure relative al Centro elaborazione dati

- I locali in cui sono posti i sistemi informatici, sono dotati di sistemi di accesso controllato, che ne impediscano l'accesso a persone non autorizzate.

Misure relative all'imputabilità

- Le operazioni effettuate sul sistema server sono registrate.

Misure relative ai supporti elettronici di memorizzazione dei dati

- I supporti utilizzati per il Disaster Recovery sono custoditi in armadi chiusi a chiave o in locali ad accesso controllato. La medesima procedura viene eseguita per tutti gli altri supporti su cui si sono memorizzati i dati trattati.

Controllo periodico dei sistemi

- Verifica semestrale, finalizzata al controllo del rispetto delle misure di sicurezza previste, ed alla convalida dell'efficacia di queste nel caso di installazione di nuove applicazioni o di modifica delle precedenti;

Verifica periodica

- verifica periodica annuale, dell'efficacia e del rispetto delle misure di sicurezza previste, per il controllo degli accessi fisici alle aree interessate al trattamento dei dati in esame.

8.2. ADEMPIMENTI PROVVEDIMENTO GARANTE PRIVACY 27 NOVEMBRE 2008 E SUCCESSIVE MODIFICHE

In attuazione di quanto disposto dal Garante della Privacy con il provvedimento *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema* del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008), integrato con il successivo provvedimento del 25 giugno 2009 *Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento* - (G.U. n. 149 del 30 giugno 2009) sono stati individuati gli amministratori di sistema delle Banche dati e la relativa pubblicizzazione è avvenuta tramite la rete intranet aziendale.

Di seguito si elencano le banche dati con l'indicazione degli amministratori autorizzati all'accesso:

Base Dati o Archivio	Server	Host	Accesso server	Accesso Host
DB_Giuridica	Halley	VM-Host09	Amministratori, Halley	Amministratori, KnowIT
Presenze	Halley	VM-Host09	Amministratori, Halley	Amministratori, KnowIT
Stipendi	Halley	VM-Host09	Amministratori, Halley	Amministratori, KnowIT
Db Anagrafe	Halley	VM-Host09	Amministratori, Halley	Amministratori, KnowIT
Db Statocivile	Halley	VM-Host09	Amministratori, Halley	Amministratori, KnowIT
DB Elettorale	Halley	VM-Host09	Amministratori, Halley	Amministratori, KnowIT
DB Albo Presidenti di seggio	Halley	VM-Host09	Amministratori, Halley	Amministratori, KnowIT
DB Albo Giudici popolari	Halley	VM-Host09	Amministratori, Halley	Amministratori, KnowIT
DB Albo scrutatori	Halley	VM-Host09	Amministratori, Halley	Amministratori, KnowIT
Db Protocollo	Halley	VM-Host09	Amministratori, Halley	Amministratori, KnowIT
Db Protocollo	Tolerant	VM-Host10	Amministratori, Etnoteam	Amministratori
DB ICI Halley	Halley	VM-Host09	Amministratori, Halley	Amministratori, KnowIT
DB Contabilità finanziaria	Civilia	VM-Host14	Amministratori, Dedagroup	Amministratori, Dedagroup
DB Economato **(solo consultazione)**	Enco	Enco	Amministratori,	Amministratori,

DB Economato	Civilia	VM-Host14	Amministratori, Dedagroup	Amministratori, Dedagroup
DB tributi TARSU/TARES	Halley	VM-Host09	Amministratori, Halley	Amministratori, KnowIT
DB Tributi COSAP	Tolerant	VM-Host10	Amministratori, Halley	Amministratori
Db Tributi PUBBLICITA	Tolerant	VM-Host10	Amministratori, Halley	Amministratori
Db Lavori pubblici	rack7	VM-Host07	Amministratori, STR	Amministratori
DB Pratiche ediliz privata	VMHOST01DMZ		Amministratori, CIP	Amministratori
db anagrafica messi	intranet		Amministratori	Amministratori
db biblioteca			Amministratori	Amministratori
Db Museo civico	pc70100	PC70199	Amministratori	Amministratori
DB Attività produttive	Sigepro	VM-Host08	Amministratori	Amministratori
DB patrimonio comunale	incasa		Amministratori, Atena	Amministratori
DB istruzione	monolito	VM-Host	Amministratori, NetDream	Amministratori
DB Anagrafica servizi sociali	icare	VMW-CP-LAN	Amministratori, Atena	Amministratori
DB avvocatura	landesk	VM-Host10	Amministratori	Amministratori
DB polizia locale			Amministratori	Amministratori
Db servizi cimiteriali	Halley	VM-Host09	Amministratori, Halley	Amministratori, KnowIT
db svp	landesk	VM-Host07	Amministratori	Amministratori
db progressione	intranetserver	VM-Host10	Amministratori	Amministratori
db merloni	intranetserver	VM-Host10	Amministratori	Amministratori
db contratti	rack7	VM-Host07	Amministratori, Atena	Amministratori
db vigile elettronico			Amministratori	Amministratori
DB URP			Amministratori	Amministratori
BD Ufficio stampa			Amministratori	Amministratori
db politiche giovanili			Amministratori	Amministratori
db Segreteria	irideweb	VM-Host11	Amministratori, CEDAF	Amministratori

Tabella 6 Tavola dei sistemi

Tutti gli accessi degli amministratori di sistema vengono registrati su un sistema centralizzato che riceve gli eventi e che, attraverso un sistema di “hashing”, non permette la loro alterazione. Il sistema inoltre aggiunge una propria marcatura temporale ad ogni evento ricevuto.
Ogni server ha installato un agente per l'invio dei proprio log al sistema centralizzato; tutti gli eventi ricevuti vengono archiviati in files settimanali e mantenuti per 55 settimane. Gli eventi relativi ai collegamenti degli amministratori di sistema vengono inoltre inseriti in uno specifico database per le successive verifiche richieste dal provvedimento.
Il responsabile dei sistemi informativo è l'unico amministratore di sistema del server di registrazione centralizzata degli eventi.

Al fine di ottemperare quanto previsto dal provvedimento è necessario che gli amministratori di sistema, se non preventivamente autorizzati dal responsabile dei sistemi informativi, si astengano

- dall'utilizzo dell'account di Administrator o di qualsiasi account di amministrazione generico mantenuto ai soli fini manutentivi
- dall'alterare, creare o cancellare altri account amministrativi
- dall'alterare o cancellare i log dei sistemi su cui si collegano
- dall'arrestare o modificare i servizi di inoltro e/o crittografia degli agenti installati
- dall'alterare il sistema di registrazione e i suoi collegamenti di rete

E' responsabilità degli amministratori di sistema l'informare il responsabile dei sistemi informativo di qualsiasi situazione che possa influire sulla corretta registrazione degli eventi sia locale che sul sistema centralizzato.
Il responsabile dei sistemi informativi manterrà apposito registro come storico delle operazioni sopra elencate da lui autorizzate.

8.3. PIANO DI CONTINUITÀ OPERATIVA (PCO) ICT

Con delibera n.30 del 04 Febbraio 2013 è stato approvato il primo Piano di Continuità Operativa ICT del Comune di Como, redatto ai sensi dell'art.50-bis del DLgs. N. 82/2005 e s.m.i., "Continuità operativa", come modificato dal DLgs. 235/10.

Per continuità operativa ICT si intende la capacità di un organizzazione di adottare, attraverso accorgimenti, procedure e soluzioni tecnico organizzative, misure di reazione e risposta ad eventi imprevisti che possono compromettere, anche parzialmente, all'interno o all'esterno dell'organizzazione, il normale funzionamento dei servizi ICT utilizzati per lo svolgimento delle funzioni istituzionali.
In tal senso la continuità operativa ICT deve, quindi, garantire la protezione dalle potenziali criticità delle funzionalità informatiche, tenendo conto delle risorse umane, strutturali, tecnologiche riferibili all'infrastruttura informatica, stabilendo le idonee misure preventive e correttive nel rispetto dei livelli prestazionali riconosciuti.

A tal fine, il perimetro di competenza della continuità operativa ICT comprende:

- le applicazioni informatiche e i dati del sistema informativo indispensabili all'erogazione dei servizi e allo svolgimento delle attività (informatiche e non);
- le infrastrutture fisiche e logiche che ospitano sistemi di elaborazione;
- i dispositivi di elaborazione hardware e software che permettono la funzionalità delle applicazioni realizzanti i servizi dell'amministrazione;
- le componenti di connettività locale e/o remota/geografica;
- ciò che serve per consentire lo svolgimento delle attività del personale informatico, sia interno all'amministrazione, sia, se presente, esterno, ma correlato al sistema informativo stesso;
- le modalità di comunicazione ed informazione al personale utilizzatore del sistema informativo all'interno dell'amministrazione e ai fruitori esterni dei servizi del sistema informativo dell'amministrazione, siano essi cittadini, imprese, altre amministrazioni;
- le misure per garantire la disponibilità dei sistemi di continuità elettrica (UPS e gruppi elettrogeni) e più in generale la continuità di funzionamento del sistema informativo;

- la gestione dei posti di lavoro informatizzati dell'amministrazione;
- i servizi previsti per l'attuazione del C.A.D. (fra cui ad es. la PEC; la firma Digitale ecc.)

Per quanto riguarda i posti di lavoro informatizzati (PDL), agli effetti della soluzione di continuità operativa è importante, tenuto conto delle caratteristiche del sistema informativo e delle applicazioni informatiche di cui deve essere garantito il funzionamento, considerare:

- il numero minimo di PDL che possa garantire la funzionalità dell'ufficio o della sede dove risiedono i PDL;
- la disponibilità di PDL di emergenza presso altri uffici o presso altre sedi dell'amministrazione;
- la disponibilità di dispositivi (workstation) alternativi, quali portatili, nello stesso ufficio o presso sedi diverse dell'amministrazione;
- la disponibilità di connettività alternativa (collegamenti ridondati, collegamenti via UMTS);
- la disponibilità di sistemi di continuità elettrica (UPS e gruppi elettrogeni).

9. PIANO PER LA FORMAZIONE

Le misure minime di sicurezza previste dal decreto legislativo 196/2003 ed analiticamente individuate dal disciplinare tecnico del decreto, prevedono la realizzazione di un piano di formazione, informazione e addestramento per gli incaricati del trattamento dei dati.
La formazione ha per oggetto le problematiche di sicurezza in generale, l'informazione i rischi individuati all'interno dell'Ente e l'addestramento l'utilizzazione degli strumenti che contrastano tali rischi.
L'intervento con riferimento ai risultati dell'Analisi del rischio effettuata sul sistema informatico ha l'obiettivo di fornire alle figure professionali interessate le necessarie conoscenze su:

- le problematiche di carattere generale inerenti la sicurezza informatica;
- la normativa specifica in materia di trattamento dei dati sensibili;
- le attività necessarie al mantenimento del livello di sicurezza;
- le procedure redatte allo scopo di garantire il rispetto delle misure minime;
- i compiti cui l'incaricato è chiamato ad attenersi durante l'attività di trattamento.

Il piano di dettaglio delle modalità e dei tempi di erogazione della formazione è stabilito dal Settore Risorse Umane.

10. TRATTAMENTI AFFIDATI ALL'ESTERNO

10.1 OBIETTIVI

Obiettivo di questo capitolo è fornire le linee guida dell'Ente per quanto riguarda la corretta gestione delle attività trasferite a terzi che comportano il trattamento di dati personali con l'indicazione sintetica del quadro contrattuale in cui tale trasferimento si inserisce, in riferimento alla protezione dei dati personali.

10.2 LINEE GUIDA

I requisisti essenziali per il raggiungimento dello scopo prefissato sono i seguenti:

- Attività delegata: contiene l'identificativo dell'attività che è stata oggetto di delega a terzi.
- Descrizione sintetica: contiene una descrizione sintetica dell'attività.
- Dati personali, sensibili o giudiziari interessati: contiene l'elenco dei dati personali, sensibili o giudiziari oggetto di trattamento per la realizzazione dell'attività delegata.
- Soggetto delegato: riporta l'identificativo della società o del consulente a cui è stato affidato l'incarico.
- Descrizione dei criteri per garantire l'adozione delle misure: perché sia garantito un adeguato trattamento dei dati è necessario che il soggetto esterno a cui viene affidato il trattamento si assuma alcuni impegni su base contrattuale.

Il soggetto cui le attività sono affidate dichiara:

- 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 adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere.
- di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare 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.