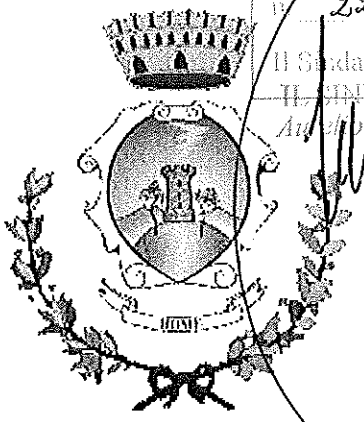
DOCUMENTO PROGRAMMATICO DELLA SICUREZZA



Allegato alla Delibera di Giunta Comunale n. 22 del 07.03.2011

Il Sindaco / Il Segretario Comunale
Arch. Alberto Allegri (Dr. Giuseppe Vitali)

COMUNE DI OME (Provincia di Brescia) - SEGRETARIO COMUNALE

Comune di OME

Provincia di Brescia

Anno 2011

01	28 Feb. 2011	Revisione Generale	Saga SpA	Amministrazione Comunale
Rev.	Data	Causale	Preparato da	Titolare Trattamento dei Dati

Indice del documento

1 Premessa

Il patrimonio informativo di ogni Amministrazione comunale rappresenta un bene di importanza fondamentale che deve essere salvaguardato garantendone l'integrità e la riservatezza. Oggi con l'avvento delle nuove tecnologie e la complessità dei sistemi informativi, il tema della sicurezza informatica, assume sempre più una rilevanza strategica. Il problema non riguarda solamente gli enormi danni causati dai virus informatici o gli attacchi provenienti dall'esterno da parte di hacker, ma anche il comportamento degli utenti ed il corretto utilizzo delle apparecchiature e degli strumenti messi a disposizione dalla tecnologia informatica. Una corretta politica di gestione della sicurezza è in grado di limitare i danni dovuti al diffondersi di informazioni riservate o a violazioni dell'integrità delle informazioni. Oltre a questi aspetti la normativa vigente in termini di privacy impone anche alle Amministrazioni che trattano dati sensibili e giudiziari di attuare una serie di misure minime per la sicurezza dei dati.

Il presente documento è stato redatto e viene tenuto aggiornato, ai sensi e per gli effetti dell'art. 31 del Decreto Legislativo 30 giugno 2003, n. 196, e tenendo conto del punto 19 dell'Allegato B "Disciplinare Tecnico in materia di misure minime di sicurezza", dal **Comune di Ome** (di seguito, per brevità, il "Titolare"). Il Documento Programmatico della Sicurezza è custodito presso l'ufficio della **Segreteria del Titolare** e riporta, in sintesi, i risultati emersi dalla valutazione e dalle misure attuate e da effettuarsi per il rispetto della normativa in materia di protezione dei dati personali vigente alla data di redazione e aggiornamento del presente documento.

2 Scopo del documento

Il presente documento costituisce il Documento Programmatico sulla Sicurezza (per brevità nel seguito denominato DPS) del Comune di Ome, la cui redazione è obbligatoria secondo i termini di legge, come prescritto dall'articolo 34 del nuovo Codice in materia di protezione dei dati (D. Lgs 196/03).

Nella redazione del presente documento, oltre a quanto prescritto dall'articolo 19 dell'allegato B), si è tenuto conto dei seguenti obiettivi:

- dare una visione il più possibile completa e dettagliata del grado di esposizione del patrimonio informativo del Comune di Ome a varie tipologie di rischi;
- individuare e mettere in atto le necessarie misure di sicurezza (organizzative, tecnologiche, logistiche, normative e procedurali) atte a garantire la protezione delle risorse (fisiche, umane, tecniche, documentali, etc.) del Comune;
- assicurare che la gestione dei dati personali e più in generale di tutti i dati importanti e sensibili del Comune di Ome avvenga con un ragionevole livello di sicurezza, riservatezza e privacy;
- dotare il Comune di Ome di un documento, redatto e certificato secondo quanto richiesto dalla normativa vigente, che permetta al Comune stesso di essere formalmente e sostanzialmente adempiente a quanto espressamente disposto dall'art. 19 dell'allegato B) del nuovo Codice, e quindi di evitare le pesanti sanzioni penali e amministrative previste.

3 Campo di Applicazione

Il presente Documento Programmatico sulla Sicurezza, previsto dalla norma attuativa (D. Lgs. 196/2003), si applica a tutti i dati trattati dal Titolare o, per incarico dello stesso, gestiti all'esterno presso terzi, sia con strumenti elettronici o comunque automatizzati che con altri strumenti e supporti, anche non elettronici.
Esso è l'atto conclusivo di una serie complessa di verifiche sullo stato della "sicurezza informatica" nel comune. L'adeguamento alla normativa, che prevede un aggiornamento dello stesso documento entro il 31 marzo di ogni anno, sarà un'occasione per effettuare una valutazione complessiva sul Sistema Informatico Comunale nel suo complesso ed eventualmente programmare miglioramenti inerenti la gestione della sicurezza. La presente procedura si applica alle sedi sotto identificate:

Denominazione sede	Ubicazione
Sede Comunale	Piazza Aldo Moro
Biblioteca	Via Maestrini 1

Questo documento stabilisce anche i compiti e le responsabilità dei soggetti che, a vario titolo e con diverse funzioni e responsabilità, sono coinvolti nel trattamento dei dati e i soggetti da questi delegati.

4 Concetti, Abbreviazioni, Definizioni

SW: software

Trattamento: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati.

Dati Personali: Qualunque informazione relativa a persona fisica, persona giuridica,ente od associazione, identificati o identificabili , anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

Dati identificativi: i dati personali che permettono l'identificazione diretta del interessato;

Dati sensibili: dati idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione ai partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dati Giudiziari: i dati personali idonei a rilevare provvedimenti di cui all'articolo 3 comma 1, lettere da a) ad o) e da r) a u) del DPR 14 novembre 2002, n 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

5 Struttura del documento

Il Documento Programmatico della Sicurezza è stato strutturato trattando i seguenti argomenti:

a) L'identificazione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
b) l'identificazione degli asset coinvolti nel trattamento dei dati
c) l'identificazione delle banche dati gestite dal comune;
d) l'analisi dei rischi che incombono sui dati;
e) le misure adottate 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;
f) la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni;
g) 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.
h) la gestione delle attività di verifica inerenti l'adozione delle misure minime di sicurezza;

5.1 Revisione dei documenti

L'emissione e la revisione del Documento Programmatico della Sicurezza, avviene nel rispetto di regole precise e sotto la sorveglianza del Responsabile dell'Area Affari Generali; ciò garantisce uno sviluppo equilibrato e congruente con l'evoluzione del sistema informativo e dell'organizzazione del Comune.

Il documento viene redatto, aggiornato e tenuto ai sensi dell'art. 34, comma 1, lett. e), D. Lgs. 30 giugno 2004, n. 196 e del punto 19 dell'Allegato B "Disciplinare Tecnico in materia di misure minime di sicurezza"

Le regole da seguire per i vari tipi di documenti sono le seguenti:
Il DPS contiene le politiche di sicurezza del Comune di Ome. Eventuali modifiche della policy e revisioni del documento possono essere suggerite per iscritto da qualsiasi collaboratore del Comune al Responsabile dell'Area Affari Generali che le valuta e decide per un'eventuale modifica.

L'analisi dei rischi identifica i possibili eventi indesiderati che possono causare un danno alle risorse del sistema informativo. Una revisione degli stessi può essere determinata da una serie di motivi, variazione dell'impianto informativo, mutate condizioni organizzative o logistiche.

Le modifiche accolte portano alla revisione del Documento Programmatico della Sicurezza. Va ribadito che l'iter di controllo e approvazione dei documenti, di cui ai punti precedenti, deve possibilmente rispecchiare quello della prima emissione, a meno di cambiamenti del personale del Comune o di cambiamenti organizzativi. Per ogni modifica effettuata si aggiorna progressivamente il numero della revisione.

La focalizzazione delle modifiche introdotte con le varie revisioni viene effettuata mediante un segno di evidenziazione del testo. Nel caso di revisione generale, i contenuti della procedura variati sono tali da considerarne una nuova impostazione.
L'aggiornamento dell'archivio cartaceo e dei file elettronici è compito del Responsabile dell'Area CED.
Quando un Documento della sicurezza è revisionato, il Responsabile dell'Area Affari Generali, conserva la copia superata in formato elettronico in un'apposita directory.

Documento	Redazione	Approvazione	Distribuzione	Archiviazione
DPS	SAGA SpA	Dirigente Comunale	Segreteria	Segreteria

6 COMPITI e RESPONSABILITÀ

Il nuovo Codice in materia di protezione dei dati prevede le seguenti figure:

- **Titolare**: ai sensi dell'art. 4, comma 1, lettera f) del D. Lgs. 196/2003, per "Titolare" si intende la persona fisica, la persona giuridica, la Pubblica Amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità e alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Nel caso delle Pubbliche Amministrazioni Locali, ed in particolare nel caso dei Comuni, il Titolare è costituito dal Comune stesso, inteso come persona giuridica. E' prassi frequente che, negli atti e nelle notifiche che richiedano una firma (come ad esempio una notifica al Garante per la protezione dei dati), che il Titolare, vale a dire il Comune stesso, sia rappresentato dal Sindaco, in qualità di legale rappresentante del Comune.

- **Responsabile del trattamento dei dati**: ai sensi dell'art. 4, comma 1, lettera g) del D. Lgs. 196/2003, si individua quale "Responsabile" la persona fisica, giuridica, la Pubblica Amministrazione o altro ente, associazione o organismo preposti dal Titolare al trattamento dei dati personali. Il responsabile è designato dal titolare facoltativamente. Il Responsabile deve essere individuato e nominato tra i soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, compreso il profilo della sicurezza. E' importante mettere in evidenza che la nomina del Responsabile del trattamento dei dati non è obbligatoria, ma consigliata nel caso di struttura complessa ed articolata in diversi uffici dell'ente. E' altresì importante mettere in evidenza le seguenti precisazioni: "ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione dei compiti", e inoltre "i compiti affidati al responsabile sono analiticamente specificati per iscritto";

- **Amministratore di sistema**: L'Amministratore di Sistema è una di quelle figure identificate anche dalla direttiva del garante del 27 novembre 2008,

come soggetto "cui è conferito il compito di sovrintendere alle risorse del sistema informativo di un ente di consentirne il buon funzionamento".
L'amministratore di sistema ha il compito di configurare gli apparati del Sistema Informativo Comunale e di definire le regole di backup delle banche dati.
E' inoltre responsabile della configurazione degli apparati e dei tool di sicurezza informatica.

- **Custode delle password**: sono i soggetti preposti alla custodia delle parole chiave (utilizzate dagli incaricati per l'accesso ai dati e dall'Amministratore di Sistema) o che hanno accesso alle informazioni che concernono le medesime; la figura del custode delle password è stata ampiamente rivalutata dal D. Lgs. 196/2003, che dedica a questa figura articolo 10 dell'Allegato B): "quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante l'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".

- **Incaricato**: "la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile"; in sintesi l'incaricato assume, in ordine al trattamento, funzioni prettamente operative ed esecutive in aderenza a specifiche istruzioni ricevute dal Titolare o dal Responsabile.
  L'articolo 30 del D.Lgs. 196/2003 specifica inoltre che:
  - "le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite",
  - "la designazione (degli incaricati) 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";

- "**Azienda esterna coinvolta nel processo di trattamento dei dati**": non è infrequente il caso in cui una parte del processo di trattamento dei dati venga svolto da un'azienda o un ente esterno. Questa casistica è stata ben individuata e normata dal nuovo Codice, che al punto 19.7, tra le informazioni che devono essere contenute nel DPS prevede "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"; questa prescrizione comporta delle significative conseguenze in termini organizzativi e pratici; infatti:
  - in caso di esternalizzazione di dati e/o processi, l'onere di individuare e mettere in atto adeguate misure di sicurezza non può essere demandato all'entità esterna: in altre parole, il titolare o responsabile non se ne può "dimenticare", ma deve assumersi la responsabilità di individuare e prescrivere contrattualmente dette misure di sicurezza, che dovranno obbligatoriamente venire adottate dalla controparte;
  - l'individuazione di adeguate misure di sicurezza non è più lasciata all'iniziativa e alla sensibilità del responsabile o del titolare, come accadeva

in precedenza; ora esiste una chiara prescrizione di legge, che in caso di non ottemperanza configura l'ipotesi di reati di mancata adozione di misure minime di sicurezza.

6.1 Figure definite dal Comune di Ome

In questo paragrafo sono evidenziate le figure formalmente definite dal Comune di Ome:

Figura prevista dalla legge	Figura definita presso il Comune di Ome	Note
Titolare del trattamento dei dati	Individuato nel Comune di Ome inteso come persona giuridica	Nel caso di una Pubblica Amministrazione il Titolare è l'entità nel suo complesso, intesa come persona giuridica (Art. 28 D. Lgs. 196/2003).
Responsabile del trattamento dei dati	Identificato nelle figure dei Responsabili di Area del comune	Nominato formalmente attraverso una lettera di incarico
Incaricato del trattamento dei dati	Figura individuata nelle persone (dipendenti o consulenti) che nell'ambito del comune trattano le banche dati.	La designazione individua puntualmente l'ambito del trattamento consentito" (Art. 30 D. Lgs. 196/2003).
Amministratore di Sistema informativo del Comune	Attualmente questa figura non è presente	
Custode delle parole chiave	Identificato nella figura del Responsabili di Area	Le password vengono custodite in un luogo sicuro.
Aziende esterne coinvolte nel processo di trattamento dei dati	Sono state inquadrate come Responsabile del trattamento dei dati.	L'obbligo di nominare le aziende e le entità esterne è stato ribadito dal nuovo Codice in materia di protezione dei dati, all'articolo 19.7 dell'allegato B) del D. Lgs. 196/2003

Nell'ambito del presente DPS, con lettere di incarico formali, saranno definiti i ruoli mancanti e saranno assegnate istruzioni e responsabilità in forma scritta, coerentemente con il dettato normativo.

6.2 Aziende esterne e fornitori di servizi

Per una gestione corretta delle problematiche connesse alla sicurezza e alla privacy, le aziende esterne (comprese quelle dove il Comune di Ome dovesse possedere una quota di partecipazione azionaria) che collaborano con l'ente nell'erogare servizi che comportano il trattamento dei dati personali e/o sensibili, devono essere inquadrate come Responsabili del trattamento dei dati da parte dei responsabili del settore al quale appartengono le banche dati oggetto di cessione o comunicazione (nel caso di banche dati "trasversali" o non direttamente riconducibili ad un ben determinato settore, la nomina dell'azienda esterna dovrà essere fatta direttamente dal titolare del trattamento dei dati, quindi dal Sindaco in qualità di Legale Rappresentante dell'Ente.

Oltre ad aziende esterne, il Comune di Ome si avvale dei servizi di consulenti, e collaboratori, come illustrato in seguito dovranno essere incaricati al trattamento dei dati.

6.2.1 Amministratori di sistema

Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

6.3 Nomina responsabili ed incaricati del trattamento dei dati

L'individuazione precisa dei vari ruoli previsti dalla legge e l'attribuzione in forma scritta di istruzioni dettagliate e di responsabilità è uno degli aspetti più critici della sicurezza organizzativa.

Come normato dal Garante per la protezione dei dati e specificato nell'articolo 30 del D. Lgs. 196/2003, "la designazione (degli incaricati) è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale, anche la documentata proposizione della persona fisica ad un'unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima".

Di seguito si riportano alcune linee guida utili per l'applicazione corretta della normativa.

Tipologia e criticità dei dati trattati

Un parametro importante è costituito dalla tipologia dei dati trattati, da quanto questi siano sensibili e da quanto elevato e fondato sia il rischio che possano avvenire trattamenti non corretti o diffusioni o accessi non autorizzati. È chiaro che all'aumentare del rischio, è ragionevole che il Responsabile sia il più analitico possibile nell'attribuzione di compiti e responsabilità, e voglia anche ragionevolmente cautelarsi da un punto di vista legale in caso di trattamenti non corretti effettuati dagli incaricati.

Omogeneità dei trattamenti effettuati

Nel caso i trattamenti siano effettuati da un'articolazione organizzativa A ben definita, e i trattamenti siano omogenei, è possibile sfruttare per la nomina la prassi "semplificata" permessa dall'articolo 30 del D. Lgs 196/2003: in altre parole non sarà necessario fare una nomina "ad personam", ma sarà sufficiente specificare analiticamente per iscritto i trattamenti consentiti all'articolazione organizzativa in questione; in questo modo tutti i dipendenti e collaboratori appartenenti all'articolazione organizzativa A sono automaticamente e correttamente nominati incaricati del trattamento dei dati. Questa prassi semplificata è particolarmente utile laddove vi sia un elevato "turn-over" di dipendenti o collaboratori.

7 Identificazione delle Risorse (asset)

Le risorse/siti che in qualche modo intervengono nella gestione e archiviazione dei dati del titolare sono identificate da:
- luoghi fisici
- apparati del sistema informativo
- software di gestione dei dati.

Di seguito verrà data una descrizione sommaria di questi elementi.

7.1 Luoghi Fisici

I luoghi fisici dove si svolge il trattamento dei dati sono identificati nel paragrafo cap 3.

7.2 Sistema Informativo

7.2.1 Server

Il sistema informativo del Comune di Ome si compone di più server.
I server principali sono collocati nell'ufficio dell'Anagrafe e della Ragioneria.
Sui server sono installate le banche dati del Comune di Ome e l'accesso ai server avviene tramite identificazione dell'utente.
Il server sono alimentati con una batterie di continuità.

Nome Server	Caratteristiche	Assegnazione
Server	SO: Windows 2003 SP3 Xeon 2.27 Ghz Ram 4 GB 3 HD 146 GB	Banche dati del demografico Alimentato da un UPS
NAS		Back-up dei dati

7.2.2 Rete informatica

La rete del comune è basata su sistema operativo Microsoft. L'accesso alla rete di internet è protetto con un Firewall.
Il comune ha una sede periferica (Biblioteca) che non è collegata alla Sala Server. In questa sede è attiva una connessione alla rete di internet usata per la connessione al WEB.

Nella tabella di seguito riportata sono identificati gli apparati principali.

Descrizione	Marca	Assegnazione
Sede Municipale		
Router Rdsl (armadio rack)	FunkWerk	Connette gli apparati della rete del comune alla rete di internet
1 Switch (armadio rack)	3Com	Connette in rete gli apparati

		del sistema informativo del comune

7.2.3 Personal Computer

I PC in dotazione ai dipendenti del Comune di Ome sono dotati di sistemi operativi windows. Le macchine sono gestite e mantenute da una società a cui è affidato il servizio di manutenzione. Su ogni PC è installato l'antivirus che si aggiorna automaticamente scaricando le impronte virali dal server.
L'accesso alla rete avviene tramite la creazione di un account composto da un identificativo e da una password.
La società incaricata della manutenzione del sistema informativo gestisce in modo controllato la configurazione dei client ed è a conoscenza di una serie di informazioni di carattere tecnico:

- SO installato
- Patch installata
- Dimensione del disco
- Ram installata
- Antivirus installato

7.2.4 Software di gestione degli uffici Software

Sono di seguito elencate gli applicativi software utilizzati per il trattamento dei dati.

Servizio/Applicativo	**Nome del software**	**Fornitore/Manuten.**
Gestione Protocollo	Sicr@web	Saga SpA
Gestione Ragioneria	Sicra	Saga SpA
Gestione Biblioteca	Sebina	Provincia di Brescia
Gestione Cimiteri	Sicra	Saga SpA
Gestione Anagrafe, elettorale, leva	Sicra	Saga SpA
Gestione ICI	Sicra	Saga SpA
Gestione Tarsu/Tia	Sicra	Saga SpA

Ci sono poi alcune soluzioni software utilizzate dai vari uffici per l'inserimento di dati o per l'espletamento di procedimenti, che sono gestite da ministeri, enti o provincie.

7.3 Classificazione dei Dati e delle Informazioni

I dati gestiti dal Comune di Ome sono stati classificati in tre tipologie:

- Dati Sensibili
- Dati Giudiziari
- Dati Personali

Per ognuno di questi sono previste diverse politiche di protezione e di salvaguardia degli stessi.

Servizi	*Ufficio*	*Tipologia di dati trattati*	*ModTrat*	*Tip. Trat*	*Nat. Trat*	*Software Applicativo/ Data Base*	*Server Supporto di memorizzazione*	Ente/ Fornitore incaricato del trattamento	*Modalità di connessione*
Affari Generali	Affari Generali / Segreteria	Gestione dati relativi a consulenza giuridica, patrocinio legale, difesa in giudizio dell'amministrazione, attività stragiudiziale e recupero debiti; consulenza e copertura assicurativa in caso di responsabilità civile verso terzi dell'amministrazione	E/D	A	P/S/G	File office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali / Segreteria	Pratiche di contenzioso relative al personale dipendente e agli amministratori in relazione al lavoro svolto per conto dell'Ente.	E/D	A	P/S/G	File office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali / Segreteria	Dati relativi agli amministratori	E/D	A	P/S/G	File office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali / Segreteria	Schede di valutazione del personale	E/D	A	P/S/G	File office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali / Segreteria	Dati relativi ai concorsi e curriculum dei partecipanti	E/D	A	P/S/G	File office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali / Segreteria	Gestione dei dati relativi a persone oggetto di interrogazioni, interpellanze mozioni, ordini del giorno, nell'ambito dell'attività ispettiva dei Consiglieri	E/D	A	P/S/G	File office	SrvOme	Fraternità e Sistemi	LAN

		Comunali;							
Affari Generali	Affari Generali / Segreteria	Gestione dei dati relativi agli organi istituzionali dell'Ente, nonché dei rappresentanti del Comune presso altri Enti	E/D	A	P/S/G	File office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali / Segreteria	Commissioni comunali	E/D	A	P/S/G	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali / Segreteria	Registrazioni del consiglio	E/D	A	P/S/G	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali / Segreteria	Delibere di Giunta	E/D	A	P/S/G	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali / Segreteria	Delibere di Consiglio	E/D	A	P/S/G	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali / Segreteria	Ordinanze del sindaco	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali / Segreteria	Corrispondenza del sindaco e segnalazione dei cittadini	E/D	A	P/S	File office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali / Segreteria	gestione dei dati di cittadini/associazioni/enti e organi vari che si rapportano con il Sindaco e con gli altri organi istituzionali.	E/D	A	P	File office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali / Segreteria	Gestione dei dati relativi a persone/associazioni per cerimonie ed incontri istituzionali	E/D	A	P	File office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali / Segreteria	gestione dei dati relativi a persone/partiti/comitati/associazioni per l'utilizzo di sale comunali per ragioni di propaganda politica e/o per incontri di varia natura	E/D	A	P/S	File office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali / Segreteria	Richieste di accesso agli atti	D	A	P				

Affari Generali	Affari Generali / Segreteria	Documenti relativi all'archivio storico e di deposito	D	C	P/S/G				
Affari Generali	Affari Generali / Segreteria	Gestione dei piani di formazione del personale dell'ente	E/D	A	P	File office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali / Segreteria	Pubblicazioni	E/D	A	P	Sicra@web	SrvOme	Saga SpA	LAN
Affari Generali	Affari Generali / Segreteria	Gestione dei dati contenuti negli atti da notificare per conto del Comune e/o di altri Enti (Registro notificazioni)	E/D	A	P	File office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali / Segreteria	Posta elettronica certificata	E/D	A	P/S/G	Casella posta certificata		Infocamere	Web
Affari Generali	Protocollo	Protocollo corrispondenza in entrata ed in uscita	E/D	A	P/S/G	Sicra@web	SrvOme	Saga SpA	LAN
Affari Generali	Affari Generali / Segreteria	Gestione archivio di deposito e archivio storico dei documenti cartacei del Comune	D	A	P/S/G				
Affari Generali	Affari Generali / Segreteria	Banca Dati inerente i contratti degli alloggi, la gestione dei relativi bandi e le procedure di assegnazione	E/D	A	P/S	File office	SrvOme	Fraternità e Sistemi Aler	LAN
Affari Generali	Affari Generali - Relazioni con il Pubblico - Servizi alla Persona	Banca Dati cimiteri	E/D	A	P	Sicra@web	SrvOme	Saga SpA	LAN
Affari Generali	Affari Generali - Relazioni con il Pubblico - Servizi alla Persona	Banca dati relativa alla pratica per la stipula dei contratti tra comune e terze parti	E/D	A	P/G	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali	Contratti	E/D	A	P/S	File di Office	SrvOme	Fraternità e	LAN

	- Relazioni con il Pubblico - Servizi alla Persona							Sistemi	
Affari Generali	Affari Generali - Relazioni con il Pubblico - Servizi alla Persona	Fascicoli personali dei dipendenti	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali - Relazioni con il Pubblico - Servizi alla Persona	Dati relativi all'inquadramento contrattuale	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali - Relazioni con il Pubblico - Servizi alla Persona	Schede valutazione del personale	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Affari Generali - Relazioni con il Pubblico - Servizi alla Persona	Dati inerenti assunzione del personale	E	A	P	Portale Provincia		Provincia	Internet
Affari Generali	Commercio	Gestione dati finalizzata al rilascio di licenze per il commercio fisso, attività di somministrazione di alimenti e bevande, l'artigianato, la pubblica sicurezza, carburanti, trasporto autobus e autovetture con conducente, stampa giornali e riviste.	E/D	A	P/G	File office	SrvOme	Fraternità e Sistemi	LAN

Affari Generali	Commercio	Dati relativi agli artigiani	E/D	A	P/G	File office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Commercio	Dati relativi agli infortuni sul lavoro	E/D	A	P/S	File office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Commercio	SUAP (dati relativi alle DIA e DIAP, gestione istanze ampli manto immobili in cui risiedono le attività produttive,)	E/D	A	P/G	File office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Commercio	Dati relativi ai pubblici esercizi	E/D	A	P/G	File office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Commercio	Dati relativi ai collaudi degli ascensori e ai titolari degli impianti	E/D	A	P	File office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Demografici	Anagrafe: gestione dati relativi all'anagrafe della popolazione residente	E/D	A	P	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Affari Generali	Demografici	Anagrafe: gestione dati relativi all'anagrafe della popolazione residente all'estero	E/D	A	P	AnagAire	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Demografici	Cartellini individuali	D	A	P	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Affari Generali	Demografici	Cartellini minori	D	A	P	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Affari Generali	Demografici	Schede di famiglia	D	A	P/S	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Affari Generali	Demografici	Carte di identità	E/D	A	P	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Affari Generali	Demografici	Passaporti	E/D	A	P	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Affari Generali	Demografici	Permessi di soggiorno	E/D	A	P/S	Sicra	SrvOme	Saga SpA	LAN

								Fraternità e Sistemi	
Affari Generali	Demografici	Anagrafe: dati relativi a immigrazione	E/D	A	P/S	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Affari Generali	Demografici	Anagrafe: dati relativi a emigrazione	E/D	A	P/S	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Affari Generali	Demografici	Stato civile: gestione dati relativi ai registri di stato civile (nascita, morte, matrimoni, cittadinanza, adozioni)	E/D	A	P/S/G	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Affari Generali	Demografici	Stato civile: riconoscimenti legittimazioni	E/D	A	P/S/G	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Affari Generali	Demografici	Stato civile: convenzioni patrimoniali	E/D	A	P	Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Demografici	Stato civile: libretti famiglia internazionali	E/D	A	P	Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Demografici	Stato civile: trasporto salme	E/D	A	P	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Affari Generali	Demografici	Stato civile: Permessi seppellimento	E/D	A	P	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Affari Generali	Demografici	Stato civile: Passaporti mortuari	E/D	A	P	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Affari Generali	Demografici	Stato civile: Cremazioni	E/D	A	P	File Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Demografici	Dichiarazioni invalidità	D	A	P/S				
Affari Generali	Demografici	Gestione dati relativi alla leva dei cittadini del comune, Ruolo Matricolari	E/D	A	P/S/G	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Affari Generali	Demografici	Gestione dati relativi all'elettorato attivo e	E/D	A	P/G	Sicra	SrvOme	Saga SpA Fraternità e	LAN

		passivo						Sistemi	
Affari Generali	Demografici	Liste generali e sezionali	E/D	A	P	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Affari Generali	Demografici	Revisioni e verbali	E/D	A	P	Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Demografici	Consultazioni elettorali e propaganda	E/D	A	P/S	Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Demografici	Tessere elettorali	E/D	A	P	Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Demografici	Gestione dati relativi alla tenuta degli albi degli scrutatori e dei presidenti di seggio	E/D	A	P/G	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Affari Generali	Demografici	Gestione dati relativi alla tenuta degli albi dei giudici popolari	E/D	A	P/G	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Affari Generali	Demografici	Schede Istat	D	A	P				
Affari Generali	Demografici	Dati del censimento	D	A	P				
Affari Generali	Demografici	Gestione dati per scopi statistici	E/D	A	P	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Affari Generali	Demografici	Cessioni di fabbricato	E/D	A	P	File office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Demografici	Pensioni	E/D	A	P/S	File office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Biblioteca	Anagrafe utenti della biblioteca	E/D	A	P	Sebina		Provincia Brescia	LAN
Finanziario	Biblioteca	Dati relativi ai prestiti dei libri	E/D	A	P/S	Sebina		Provincia Brescia	LAN
Finanziario	Biblioteca	Dati relativi all'anagrafica degli incaricati dal comune per la realizzazione di attività e alle manifestazioni culturali	E/D	A	P	File di Office	PC biblioteca	Fraternità e Sistemi	LAN
Finanziario	Cultura	Dati relativi alle Associazioni ed	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN

		organizzazioni di Volontariato che chiedono l'iscrizione all'albo comunale.							
Finanziario	Cultura	Dati relativi a persone/associazioni per il conferimento di onorificenze e ricompense, per la concessione di patrocini e premi di rappresentanza, per l'adesione a comitati d'onore e l'ammissione a cerimonie ed incontri istituzionali	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Cultura	Dati relativi a persone/associazioni per l'organizzazione di manifestazioni culturali e sportive	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Cultura	Dati relativi ad aziende o enti che collaborano con il Comune per la realizzazione di iniziative culturali e sportive	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Cultura	Dati relativi a persone incaricate dal Comune per la realizzazione di eventi culturali e sportivi	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Istruzione	Dati relativi agli alunni che usufruiscono della mensa scolastica e delle rispettive famiglie, qualora si evincano dati sensibili legati a convinzioni religiose e/o filosofiche delle famiglie stesse	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN

Finanziario	Istruzione	Dati relativi alle rette inerenti i servizi scolastici e solleciti di pagamento	E/D	A	P/S	Applicativo personalizzato	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Istruzione	Bandi per l''assegnazione di borse di studio	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Istruzione	Domande relative alla dote scuola	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Istruzione	Gestione degli impianti sportivi delle scuole	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Istruzione	Dati relativi agli alunni che usufruiscono del trasporto scolastico	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Istruzione	Dati relativi al reddito (certificazione ISEE) delle famiglie che chiedono i contributi per i libri scolastici dei figli	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Istruzione	Corrispondenza con gli istituti scolastici	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi alle gare di appalto	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Anagrafica associazionismo e volontariato	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi all'ISEE	D	A	P/S	Portale Inps	Portale Inps		internet
Finanziario	Servizi Sociali	Cartelle utenti	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi all'assegno maternità	E	A	P/S	ISEE	Portale Inps		Internet
Finanziario	Servizi Sociali	Banca Dati Siatel	E	B	P/S	Portale	Portale Ministero entrate		Internet
Finanziario	Servizi Sociali	Dati relativi all'assegno	E	A	P/S	Portale	Portale Regione		Internet

		nuclei numerosi				Regione Lombardia	Lombardia		
Finanziario	Servizi Sociali	Dati relativi alle famiglie indigenti	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi agli utenti dei servizi alla persona	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi alle pratiche di assistenza domiciliare	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi all'assistenza scolastica ai portatori di handicap o con disagio psico-sociale	E/D	A	P/S/G	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi alle richieste di ricovero o inserimenti in Istituti, Case di cura, Case di Riposo	E/D	A	P/S/G	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi alla concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti gravemente disabili)	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi agli utenti che usufruiscono di centri diurni, socio-educativi	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi a persone bisognose o non autosufficienti che usufruiscono del trasporto pubblico	E/D	A	P/S	File di Office	SrvOme	Associazione incaricata del servizio Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi ai canoni di locazione	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi alla prevenzione e al sostegno alle persone tossicodipendenti e alle	E/D	A	P/S/G	File di Office	SrvOme	Fraternità e Sistemi	LAN

		loro famiglie tramite centri di ascolto e centri documentali							
Finanziario	Servizi Sociali	Dati relativi all'assistenza nei confronti di minori	E/D	A	P/S/G	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi alla concessione di benefici economici	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati inerenti i piani di Zona	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi ai progetti presentati nell'ambito della legge regionale 328	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Sostegno nucleo famigliare e affido minori	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Assistenza scolastica ad personam	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Pratiche relative all'integrazione sociale e all'istruzione del portatore di handicap e di altri soggetti con disagio sociale	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Trattamenti sanitari obbligatori	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi agli utenti della casa di riposo	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi agli inabili al lavoro	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi al bonus	E/D	A	P	File di Office	SrvOme		LAN

		SGATE						Fraternità e Sistemi	
Finanziario	Servizi Sociali	Dati relativi ai contributi per affitto	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi alle cooperative sociali con le quali il comune collabora	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Contributi ad enti ed associazioni	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Dati relativi alle commissioni comunali	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Anagrafica professionisti che collaborano con il settore	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Servizi Sociali	Atti di liquidazione	E/D	A	P	File di Office	SrvOme		LAN
Finanziario	Ragioneria	Dati relativi alle entrate del Comune,	E/D	A	P	Sicra	SrvOme	Saga spA	LAN
Finanziario	Ragioneria	Dati relativi ai fornitori e ai professionisti che collaborano con l'ente	E/D	A	P	Sicra	SrvOme	Saga spA	LAN
Finanziario	Ragioneria	Dati contabili e fiscali dell'Ente	E/D	A	P	Sicra	SrvOme	Saga spA	LAN
Finanziario	Ragioneria	Fatture fornitori	D	A	P	Sicra	SrvOme	Saga spA	LAN
Finanziario	Ragioneria	Mandati e reversali	E/D	A	P	Sicra	SrvOme	Saga spA	LAN
Finanziario	Ragioneria	Dati contabili relativi agli amministratori, incarichi professionali, dipendenti, enti, fornitori ed associazioni	E/D	A	P	Sicra	SrvOme	Saga spA	LAN
Finanziario	Ragioneria	Denuncia 770	E/D	A	P	Sicra	SrvOme	Saga spA	LAN
Finanziario	Ragioneria	Economato: gestione dei	E/D	A	P	Sicra	SrvOme	Saga spA	LAN

		beni mobili di proprietà comunale							
Finanziario	Ragioneria	Economato: dati delle aziende fornitrici ed impegni di spese	E/D	A	P	Sicra	SrvOme	Saga spA	LAN
Finanziario	Personale	Anagrafica dipendenti con contratto a tempo determinato amministratori borsiti e co.co.pro.	E/D	A	P	File di Office	SrvOme	LP SERVICE Fraternità e Sistemi	LAN
Finanziario	Personale	Dati relativi all'inquadramento contrattuale	E/D	A	P	Office	Comune-srv3	LP Service Fraternità e Sistemi	LAN
Finanziario	Personale	Dati inerenti i cedolini paga	E/D	A	P	File di Office	SrvOme	LP Service Fraternità e Sistemi	LAN
Finanziario	Personale	Dati relativi alle denunce mensili imponibili, CPDEL e Inadel	E/D	A	P	File di Office	SrvOme	LP Service Fraternità e Sistemi	LAN
Finanziario	Personale	Dati relativi alle gestione dei benefici per invalidità	E/D	A	P	File di Office	SrvOme	LP Service Fraternità e Sistemi	LAN
Finanziario	Personale	Dati relativi alle denunce fiscali e previdenziali	E	A	P/S	File di Office	SrvOme	LP Service Fraternità e Sistemi	LAN
Finanziario	Personale	Gestione permessi e aspettative sindacali	E	A	P/S	File di Office	Server3	Fraternità e Sistemi	LAN
Finanziario	Personale	Gestione 730	E	A	P	File di Office	SrvOme	LP Service Fraternità e Sistemi	LAN
Finanziario	Personale	Gestione 770	E	A	P	File di Office	SrvOme	LP Service Fraternità e Sistemi	LAN
Finanziario	Personale	Contributi previdenziali	E	A	P	Portale INPS	SrvOme	LP Service	LAN e

								Fraternità e Sistemi	internet
Finanziario	Personale	Banca dati previdenziali	E	A	P/S	Portale INPDAP		INPDAP	Internet
Finanziario	Personale	Denunce Infortunio	E	A	P/S	Portale INPS		INPS	Internet
Finanziario	Personale	Dati relativi ai permessi sindacali ed aspettative	E	A	P/S	Gedap		Ministero della Funzione Pubblica	Internet
Finanziario	Tributi	Anagrafica contribuenti Codici fiscali e posizioni tributarie	E	C	P	Siatel	Web	Ministero delle Finanze	Internet
Finanziario	Tributi	Dati catastali	E	B	P	Sister	Web	Agenzia territorio	Internet
Finanziario	Tributi	Gestione ruoli coattivi	E	A	P		SrvOme	Equitalia SpA	LAN
Finanziario	Tributi	Dichiarazione e versamenti ICI	D	A	P	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Finanziario	Tributi	Dati relativi alla Pubblicità e alle pubbliche affissioni	D	A	P	Servizio in outsourcing		Ica Srl	
Finanziario	Tributi	Accertamenti ICI e pratiche di ricorso	E/D	A	P	File di Office		Fraternità e Servizi	LAN
Finanziario	Tributi	Dichiarazione e versamenti TIA/TARSU	E/D	B	P	Sicra	SrvOme	Saga SpA Fraternità e Sistemi	LAN
Finanziario	Tributi	Autorizzazioni occupazione suolo pubblico	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Finanziario	Tributi	Cessione di fabbricati	E/D	A	P/S	File di Office	SrvOme	Equitalia SpA	LAN
Finanziario	Tributi	Banca Dati Catasto	E	B	P	Portale	Portale Catasto	Agenzia del Territorio SISTER	Internet
Tecnica	LLPP	Dati relativi alle aziende e ai professionisti che svolgono attività per conto dell'ufficio	E/D	A	P/g	File di Office	SrvOme	Fraternità e Sistemi	LAN

Uff. Tecnico	LLPP	Svincolo polizze fidejussorie	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	LLPP	Gestione dati relativi ai beni immobili di proprietà comunale	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	LLPP	Predisposizione relazioni tecniche contenenti dati relativi a persone che hanno subito danni fisici per i quali il Comune è chiamato a rispondere	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	Atti Ordinatori e prescrittivi	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	Procedimenti di acquisizione patrimoniale	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	Frazionamenti	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	Corrispondenza con notai Atti notarili	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	Corrispondenza con enti vari Asl, Arpav, Catasto, Conservatoria	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	Gestione dati inerenti pareri interni per attività trasversali (Polizia Municipale, Urbanistica)	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	Gestione dati permessi di costruzione, DIA	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	PRG, PGT, Piani Urbanistici attuativi, CDU	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	Abusi edilizi e sanzioni amministrative	E/D	A	P/G	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	Espropri	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	Ordinanza di demolizione	E/D	A	P/G	File di Office	SrvOme	Fraternità e Sistemi	LAN

Uff. Tecnico	Edilizia Residenziale	Gestione dati relativi alle pratiche di condono edilizio	E/D	A	P/G	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	Denunce deposito cementi armati	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	Pratiche antisismiche	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	Denunce deposito frazionamenti	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	Certificati di agibilità, attestazioni di silenzio-assenso	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	Svincolo polizze fidejussorie	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	Autorizzazioni paesaggistiche	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	Nulla osta igienico sanitari	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Edilizia Residenziale	Domande contributi abbattimento barriere architettoniche	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Ambiente	Valutazioni impatto ambientale	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Ambiente	Valutazione integrata ambientale	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Ambiente	Autorizzazione impianti telecomunicazione	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Ambiente	Dati relativi alle aziende che si occupano della manutenzione del verde	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Ambiente	Dati relativi a reati ambientali e relative sanzioni o ordinanze	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Uff. Tecnico	Ambiente	Dati relativi alle aziende agricole	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia	Protocollo in uscita	E/D	A	P/G	Sicr@web	SrvOme	Fraternità e	LAN

	Municipale	dell'ufficio						Sistemi	
Affari Generali	Polizia Municipale	Notizie di reato	E/D	A	P/G	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia Municipale	Denunce	E/D	A	P/G	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia Municipale	Illeciti penali	E/D	A	P/G	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia Municipale	Atti di polizia giudiziaria	E/D	A	P/G	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia Municipale	Dati relativi ai incidenti stradali	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia Municipale	Pratiche rilascio permessi passi carrai	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia Municipale	Dichiarazioni consistenza alloggi per il ricongiungimento familiare	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia Municipale	Pratiche rilascio permessi di sosta portatori di handicap	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia Municipale	Banca dati sanzioni codice della strada	E/D	A	P/G	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia Municipale	Banca dati procedure sanzionatorie	E/D	A	P/G	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia Municipale	Trattamenti sanitari obbligatori	E/D	A	P/S	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia Municipale	Trasporti eccezionali	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia Municipale	Attività relativi al rilascio delle licenze, autorizzazioni ed altri titoli abitativi previsti dalla legge.	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia Municipale	Gestione pratiche relative all'occupazione del suolo pubblico	E/D	A	P/G	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia	Dati relativi alle attività	E/D	A	P/G	File office	SrvOme	Fraternità e	LAN

	Municipale	commerciali su aree pubbliche						Sistemi	
Affari Generali	Polizia Municipale	Ordinanze	E/D	A	P/S/G	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia Municipale	Ingiunzioni del sindaco	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia Municipale	Illeciti amministrativi	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia Municipale	Pratiche vigilanza edilizia ambientale e sanitaria	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	Polizia Municipale	Contratti e convenzioni	E/D	A	P	File di Office	SrvOme	Fraternità e Sistemi	LAN
Affari Generali	CED	Banche dati elettroniche del comune	E/D	A	P/S/G	Applicativi Software di gestione del Comune	Server e pc del sistema informativo del comune	Fraternità e Sistemi	LAN

Modalità trattamento
E: Elettronico
D: Documentale

Tipo di trattamento:
A: Lettura; scrittura, salvataggio
B: Lettura, Scrittura
C: Lettura

Natura dati Trattati
P: personali
S: Sensibili
G: Giudiziari

8 Analisi dei rischi

L'analisi dei rischi è stata condotta secondo le dimensioni di analisi previste dalla normativa vigente e dalla conoscenza del contesto specifico del Comune di Ome. I rischi sono stati analizzati e valutati secondo i seguenti criteri:

- analisi dei rischi sugli aspetti organizzativi e normativi;
- analisi dei rischi sui luoghi fisici;
- analisi dei rischi sulle risorse hardware;
- analisi dei rischi sulle risorse software;
- analisi dei rischi sulle risorse dati.

E' importante mettere in evidenza che nell'analisi dei rischi sono state tenute presenti non solo le misure minime di sicurezza previste dalla legge, ma tutte le possibili misure di sicurezza necessarie in rapporto alla specifica situazione del Comune di Ome. Solo in questa maniera, in caso di "incidenti" o di verifiche ispettive, il Titolare o il Responsabile potrà fornire la prova liberatoria di cui all'articolo 2050 del Codice Civile, e potrà quindi dimostrare di avere ragionevolmente adottato tutte le misure idonee ad evitare il danno, in relazione alla specifica contingente situazione.

8.1 Analisi dei rischi sugli aspetti organizzativi e normativi

Codice rischio	Elemento di rischio	Livello di rischio	Motivazione del livello di rischio
RAO-01	Rischi di sanzioni, inadempienze e trattamenti non corretti e non conformi dovuti alla mancata individuazione e nomina degli Incaricati del trattamento dei dati.	Medio	Alla maggior parte delle aziende esterne sono state formalizzati gli incarichi inerenti il trattamento dei dati I dipendenti del comune non sono stati incaricati per il trattamento delle banche dati e sono state fornite delle istruzioni sulle regole di gestione delle risorse del sistema informativo comunale.
RAO-02	Rischi di trattamenti non corretti e non conformi dovuti alla mancata redazione di norme e istruzioni scritte e dettagliate ad uso degli incaricati del trattamento dei dati.	Basso	Per gli incaricati sono stati fatti dei corsi di formazione inerenti le regole di utilizzo delle risorse del sistema informativo e la "Legge sulla privacy"
RAO-03	Rischi di trattamenti non corretti e non conformi a causa della mancata specificazione per iscritto dell'ambito del trattamento consentito.	Basso	E' stato specificato l'ambito del trattamento consentito. L'accesso alle banche dati è profilato correttamente. E' stato adottato da parte del comune un regolamento per l'uso delle risorse del sistema informativo comunale.

RAO-04	Rischi di trattamenti non corretti e non conformi dovuti alla mancata designazione e nomina dei Responsabili del trattamento dei dati	Basso	I Responsabili e gli incaricati del trattamento dei dati non sono stati designati e nominati. L'accesso alle banche dati è profilato correttamente
RAO-05	Rischi di trattamenti non corretti e non conformi dovuti al mancato aggiornamento dei compiti, delle responsabilità e delle istruzioni che i responsabili del trattamento dei dati devono eseguire.	Basso	I compiti affidati ai Responsabili non sono stati "analiticamente specificati per iscritto" (Art. 29 D.Lgs. 196/2003).
RAO-06	Rischi di sanzioni, inadempienze e trattamenti non corretti e non conformi dovuti alla mancata nomina e responsabilizzazione dell'Amministratore di Sistema.	Basso	E' stata identificata la figura dell'amministratore del sistema informativo La gestione dell'applicativo della biblioteca è stato assegnato alla Provincia il cui tecnico è stato nominato amministratore di data base
RAO-07	Rischi di sanzioni, inadempienze e trattamenti non corretti e non conformi dovuti alla mancata nomina e del Custode delle Password.	Basso	Non tutte le password di accesso agli applicativi di gestione sono conformi a quanto indicato dal D. Lgs 196/03 Le password NON sono conservate dal custode delle password.
RAO-08	Rischi di sanzioni, denunce e trattamenti non corretti e non conformi dovuti all'assenza di un Regolamento per la privacy e la sicurezza dei dati sensibili.	Basso	E' stato adottato il regolamento per il trattamento dei dati sensibili, come richiesto dal D. Lgs 135/99 e ribadito dal D. Lgs 196/2003.
RAO-09	Rischi di sanzioni e trattamenti non conformi dovuti alla mancata individuazione e nomina delle aziende e del personale esterno coinvolto nel processo di trattamento dei dati.	Medio	Non tutte le aziende esterne che trattano i dati per conto del comune sono state nominate come responsabili del trattamento dei dati.

8.2 Analisi dei rischi sui luoghi fisici

Codice rischio	Elemento di rischio	Livello di rischio	Motivazione del livello di rischio
RLF-01	Possibilità di accesso ai documenti e agli armadi che contengono documentazione con dati personali (ci si riferisce agli armadi non presso il CED – ma agli armadi e agli archivi presso gli altri uffici del Comune).	Medio	Non tutti Gli armadi sono dotati di serratura con chiave. Il fax del comune è posizionato nell'ufficio del protocollo che è presidiato dal dipendente dell'ufficio. I dipendenti del comune chiudono a chiave gli uffici al termine dell'orario di lavoro.
RLF-02	Allagamenti edifici del comune	Basso	In passato non si sono mai verificati episodi di allagamento.
RLF-03	Incendio palazzo comunale	Basso	Non sono presenti apparati per la rilevazione del fumo presso archivio di deposito. L'impianto elettrico del comune rispetta le normative di legge. Nelle sedi del comune sono installati estintori in posti ben visibili che sono regolarmente manutenuti.
RLF-04	Incendio ufficio che ospita il server	Basso	Nel locale non sono presenti materiali infiammabili In prossimità della sala server è presente un estintore. L'edificio del comune è a norma per quanto riguarda la sicurezza nei luoghi di lavoro
RLF-07	Incendio Biblioteca	Basso	L'impianto elettrico del comune rispetta le normative di legge. Nelle sedi del comune sono installati estintori in posti ben visibili che sono regolarmente manutenuti.

			Il personale del comune ha partecipato ai corsi sulla sicurezza nei luoghi di lavoro. Nella biblioteca non sono attivi dei rilevatori di fumo
RLF-08	Terremoto.	Basso	Il Comune non si trova in una zona ad elevato rischio sismico.
RLF-09	Impossibilità o difficoltà a rilevare accessi non autorizzati ai locali del Comune dove sono custoditi documenti cartacei contenenti dati personali e dati sensibili.	Basso	Gli uffici del comune sono continuamente presidiati, non vi sono locali incustoditi o spazi accessibili al pubblico in cui sono depositati documenti.

8.3 Analisi dei rischi sulle risorse hardware

Codice rischio	Elemento di rischio	Livello di rischio	Motivazione del livello di rischio
RRH-01	Possibilità di danneggiare o mettere fuori uso le risorse hardware del palazzo comunale	Medio	Il server del comune è installato in un locale che non è chiuso a chiave. Nello stesso spazio è presente un fotocopiatore.
RRH-02	Probabilità/frequenza di guasti nelle apparecchiature hardware.	Basso	Non sono stati rilevati episodi di guasti anomali o sospetti nelle apparecchiature hardware, che risultano essere di buona qualità ed elevata affidabilità. I server principali sono alimentati con batterie di continuità in grado di limitare gli sbalzi di tensione. Gli apparati di rete non sono alimentati e protetti da batterie di continuità in grado di stabilizzare la

			tensione elettrica di alimentazione. Il server su cui sono stati installati gli applicativi di gestione del comune hanno configurazioni RAID Relativamente ai personal computer identificati come critici vengono fatte giornalmente delle immagini che sono salvate su un secondo disco installato nel PC.
RRH-03	Probabilità di mancanza oppure di discontinuità nell'alimentazione elettrica.	Basso	I server, è alimentato da batterie di continuità. Eventi di assenza prolungata dell'alimentazione elettrica sono bassi.
RRH-04	Possibilità di asportare/manomettere le unità disco.	Basso	Tutte le unità a backup sono custodite in una cassaforte questo fatto assicura una adeguata protezione.
RRH-05	Possibilità di asportare/manomettere i supporti utilizzati per le copie di backup.	Basso	I supporti utilizzati per il backup sono custoditi in un luogo sicuro diverso dalla Sala Server
RRH-06	Grave danno agli apparati o ai locali che ospitano la sala server	Basso	Un apparato di backup è installato in un locale diverso dalla sala server.
RRH-07	Possibilità di intrusioni ed accessi non autorizzati all'interno della rete locale e dei server, dovuti a scarsa efficacia della protezione fornita dal firewall	Basso	Il livello di protezione fornito dal firewall è adeguato. La rete della Biblioteca che non è protetta da firewall ma è separata dalla rete del palazzo comunale
RRH-08	Possibilità di intrusioni e accessi non autorizzati all'interno della rete locale e dei server.	Basso	La connessione remota da parte delle software house che eseguono attività di assistenza è autorizzato e supervisionato dal responsabile del sistema informativo,
RRH-09	Possibilità di intrusioni e accessi non autorizzati alla rete locale dovuti alla presenza di collegamenti ad	Basso	Il firewall fornisce un'adeguata protezione perimetrale. Su ogni pc è installato un antivirus regolarmente aggiornato.

	Internet ed all'utilizzo della posta elettronica.		I dipendenti sono stati sensibilizzati sulle tecniche utilizzate per gli attacchi informatici.

8.4 Analisi dei rischi sulle risorse software

Codice rischio	Elemento di rischio	Livello di rischio	Motivazione del livello di rischio
RRS-01	Accesso non autorizzato alle basi dati utilizzate dai software istituzionali regolarmente installati con licenza e manutenzione.	Medio	La disattivazione di user-id, a seguito di dimissioni, trasferimenti e cambio di mansioni di dipendenti e collaboratori del Comune spesso non viene eseguita tempestivamente e secondo un processo strutturato. Le password di accesso alla rete non rispettano le prescrizioni della normativa della privacy L'accesso al sw gestionale rispetta le indicazioni definite nel D. lgs 196/03
RRS-02	Presenza di anomalie e difetti software che minacciano l'integrità dei dati.	Basso	Il software installato è mediamente di buona qualità e non presenta anomalie particolarmente gravi e bloccanti.
RRS-03	Possibilità di incorrere in sanzioni per utilizzo di software non regolarmente acquistato e licenziato.	Medio	Gli utenti finali hanno la possibilità di installare e disinstallare autonomamente dei programmi, anche senza regolare licenza e autorizzazione. A tale proposito sono state date precise disposizioni in merito alla procedura da seguire per installare nuove soluzioni software.
RRS-04	Possibilità di perdita di dati a causa di virus o codici maligni.	Basso	Il rischio è molto basso, in quanto sono utilizzati degli antivirus regolarmente aggiornati installati sui client della rete informatica

RRS-05	Non conformità rispetto a quanto prescritto dall'Allegato B) del D. Lgs. 196/2003 (es. disattivazione automatica dopo sei mesi di mancato utilizzo, etc.).	Basso	Non sono state rilevate casistiche gravi di non conformità rispetto ai requisiti imposti dal D. Lgs. 196/2003. Solo in alcuni casi è stato verificato che non sempre in caso di dimissioni, trasferimenti, cambi di mansione etc., viene fatta la disabilitazione della user-id di accesso ai portali di enti esterni usati dai dipendenti del comune (Portale Regione Lombardia, Sister...ecc) questo anche a causa di una politica di gestione degli account, che richiederebbe la sottoscrizione di un nuovo accordo con l'ente stesso.

8.5 Analisi dei rischi sulle risorse dati

Codice rischio	Elemento di rischio	Livello di rischio	Motivazione del livello di rischio
RRD-01	Accesso non autorizzato alle risorse cartacee custodite presso l'Archivio Generale.	Medio	L'Archivio Generale (così come gli altri archivi "centralizzati") è chiuso, l'accesso è consentito agli addetti o al personale autorizzati. I dati depositati presso l'archivio non sono conservati in armadi dotati di serratura.
RRD-02	Accesso non autorizzato ai documenti cartacei custoditi negli archivi dei vari Settori.	Medio	Non tutti i documenti contenenti dati sensibili sono custoditi in armadi chiusi a chiave.
RRD-03	Accesso non autorizzato alle risorse dati in formato elettronico.	Basso	Non sono state rilevate casistiche gravi di non conformità rispetto ai requisiti imposti dal D. Lgs. 196/2003. Solo in alcuni casi è stato verificato che non sempre in caso di dimissioni, trasferimenti, cambi di mansione etc., viene fatta la disabilitazione della user-id di accesso ai portali di enti esterni

			usati dai dipendenti del comune (Portale Regione Lombardia, Sister ... ecc.) questo anche a causa di una politica di gestione degli account, che richiederebbe la sottoscrizione di un nuovo accordo con l'ente stesso.
RRD-04	Cancellazione/modifica non autorizzata alle risorse dati in formato elettronico.	Basso	I file di office dei vari uffici sono salvati in cartelle ad accesso selezionato salvate su server.
RRD-05	Asportazione delle unità disco nelle quali sono memorizzati i dati in formato elettronico.	Basso	Le risorse hardware principali sono ospitate in un locale dedicato, tenuto di norma chiuso a chiave.
RRD-06	Incapacità o difficoltà a ripristinare copie di backup.	Basso	Il processo di backup va sempre a buon fine. Si dovrebbero pianificare delle prove di restore delle banche dati
RRD-07	Rischi di sanzioni e trattamenti non corretti dovuti all'assenza di un piano formale di disaster recovery e di business continuity	Basso	E' stato formulato un piano di Disaster recovery, così come richiesto dal punto f) dell'art. 34 del D. Lgs. 196/2003 che tiene conto delle risorse e delle apparecchiature a disposizione dell'ente.
RRD-08	Difficoltà ad accedere ai dati tempestivamente in caso di situazioni di emergenza.	Basso	Sono stati nominati i custodi delle password, per cui in situazioni di assenza del personale titolare dell'accesso alla banca dati è possibile accedere alle banche dati del comune. Tutti gli uffici salvano i dati sul server. L'accesso alle varie banche dati è condiviso tra le persone dello stesso ufficio in base agli incarichi di trattamento dei dati.
RRD-9	Rischi derivanti dalla mancata separazione dei dati (in formato cartaceo) riguardanti lo stato di salute e la vita sessuale.	Basso	I certificati medici verranno consegnati al medico del lavoro come da recente disposizione normativa.

RRD-10	I dati (in formato elettronico) sensibili e giudiziari non sono cifrati o gestiti con codici che li rendano "anonimi"	Medio	Dalle analisi effettuate non risulta essere adottata nessuna tecnica di cifratura per la protezione dei dati sensibili.
RRD-11	Accesso non autorizzato ai dati da parte dell'amministratore di sistema	Medio	Sono stati attivati servizi che consentono di tracciare le attività dell'amministratore di sistema dato che nel comune non vi è questo tipo di figura professionale. Gli utenti con il profilo di amministratore di sistema possono accedere ai log registrati dai sistema operativo del PC o dle server

9 Piano di Sicurezza

Nell'ambito del Comune di Ome sono adottati una serie di procedimenti organizzativi volti a migliorare la sicurezza del sistema informativo.
Innanzitutto sono stati identificati i ruoli e le responsabilità delle figure professionali che nell'ambito dell'ente trattano dati.
Le figure professionali identificate verranno formalmente incaricate attraverso una delega scritta che definisce competenze e responsabilità relative alla gestione del sistema informativo e al trattamento dei dati.
Le strutture all'interno dell'organizzazione complessiva del Comune, che si occupano del trattamento di dati personali, anche in relazione ai compiti loro assegnati, sono state individuate in base alla tipologia, all'entità, alla distribuzione e all'organizzazione delle attività svolte all'interno dell'ente:

- a tale scopo ciascun dipendente e collaboratore è incaricato ed autorizzato al trattamento dei diversi tipi di dati; gli incarichi - così come la responsabilità per la conservazione dei dati vengono conferiti personalmente al momento dell'inserimento di una nuova figura all'interno della struttura dell'ente;
- ciascun incaricato può operare, per il trattamento dei dati, esclusivamente all'interno delle mansioni assegnate e in riferimento alle informazioni ed alle Banche dati disponibili relative alla propria categoria di appartenenza;
- i soggetti che trattano dati riferiti all'attività del Comune che, per qualifica attribuita od in relazione alla concreta attività svolta, non rivestono la figura di incaricati, sono stati opportunamente autorizzati al trattamento mediante specifica Convenzione.

Per quanto riguarda il Consiglio Comunale e la Giunta; tali organi non hanno poteri diretti di gestione delle banche dati, né operano eseguendo operazioni di elaborazione; tuttavia, al fine di svolgere appieno il mandato loro conferito, il sindaco, gli assessori e i consiglieri possono consultare ogni documento, sia cartaceo che informatico, anche contenente dati sensibili;

Società e ditte che effettuano la manutenzione dei Personal computer, dei software e delle reti informatiche e/o elaborazione dati. Tali soggetti operano in base a specifica autorizzazione, recante nel dettaglio i compiti e i limiti nell'espletamento dell'attività di assistenza. In particolare queste Ditte si trovano nella situazione di dover periodicamente svolgere lavori di manutenzione o, semplicemente, di verifica del funzionamento di un programma o di un'attrezzatura informatica. A tal fine è praticamente obbligatorio accedere alla banca dei dati presenti sui personal computer o all'interno dei programmi software, evidenziando una conoscenza di dati personali che di per sé non è collegata allo scopo per cui la Ditta effettua la propria attività.

Ai sensi del punto 25 del Disciplinare Tecnico allegato al D. Lgs. 196/2003, se l'adozione delle misure minime di sicurezza viene affidata a soggetti esterni alla propria struttura, quali i fornitori di programmi software dedicati, il Titolare del trattamento riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del Disciplinare Tecnico del Testo unico sul trattamento dei dati.

9.1 Audit della sicurezza

E' stato predisposto un piano di audit per verificare periodicamente, almeno una volta all'anno, l'efficacia delle misure adottate e per rivedere l'analisi dei rischi. Il dettaglio è riportato nel capitolo 12 del presente documento.

9.2 Formazione

Sono previsti dei piani di formazione per istruire i collaboratori sulle problematiche relative alla sicurezza e al trattamento dei dati. Oltre a questo aspetto verrà consegnato ai dipendenti del Comune di Ome, che effettuano trattamento di dati, una guida contenente le istruzioni per una corretta gestione delle risorse del sistema informativo. Per alcuni dipendenti comunali sono già stati fatti corsi di formazione inerenti la privacy e la sicurezza dei dati.

9.3 Gestione profili di autorizzazione

Il Comune di Ome ha adottato un procedimento che prevede la comunicazione al Responsabile dei Sistemi Informativi delle variazioni delle mansioni o dell'organico dell'ente, da parte dell'ufficio del personale o dei responsabili di settore.
Il Responsabile dei Sistemi Informativi dovrà preoccuparsi di aggiornare i diritti di accesso alle risorse del sistema informativo e ai dati trattati in modo elettronico. Periodicamente, e comunque almeno annualmente, Il Responsabile dei Sistemi Informativi verifica la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

9.4 Assunzione del personale da parte del comune

Nel caso di nuove assunzioni di personale da parte del comune si deve procedere alla profilazione dell'utente per l'accesso alle banche dati.
In particolare:

- Il responsabile di area o di Settore deve provvedere alla nomina del dipendente a incaricato o responsabile del trattamento dei dati.
- L'ufficio del personale deve consegnare al dipendente le regole per l'utilizzo del sistema informativo.
- La società che si occupa della manutenzione del sistema informativo provvedere a profilare l'utente in modo che possa accedere alle informazioni in funzione del profilo di autorizzazione.

9.5 Gestione e comunicazione dell'Informativa

Come previsto nell'articolo 13 del D. Lgs 196/2003 il comune di Ome ha predisposto delle informative rivolte alle diverse categorie di soggetti interessati:

- Cittadini
- Dipendenti del comune
- Fornitori / Enti / Associazioni

L'informativa è stata pubblicata, presso i vari uffici e gli sportelli a cui il pubblico accede abitualmente.
Relativamente ai dipendenti del comune l'informativa è stata consegnata dall'ufficio del personale e firmata dai dipendenti per presa visione.
Sul sito internet del comune è stata creata un'area relativa alla "legge sulla privacy" all'interno della quale è stata pubblicata l'informativa sul trattamento dei dati.

9.6 Sicurezza Fisica

La politica della sicurezza identifica i comportamenti che regolano l'accesso fisico a luoghi in cui sono conservati o custoditi dati personali o sensibili. A tale proposito si può identificare una classificazione degli stessi in:

- Aree ad accesso non controllato
- Aree ad accesso controllato
- Aree ad accesso ristretto

Per ognuna di queste sono state definite delle modalità di gestione degli accessi e delle regole per quanto riguarda l'installazione delle apparecchiature.

9.6.1 Controllo degli accessi agli edifici

Le sedi del Comune di Ome in cui viene effettuate il trattamento dei dati sono identificate nel paragrafo 3. di seguito vengono identificate le misure di sicurezza fisiche adottate per la protezione delle banche dati e degli strumenti di elaborazione.

Denominazione sede	Sistema Sicurezza	Antincendio	Accesso all'edificio
Sede Municipale Disposta su due piani	Le finestre del piano terra sono protette con delle inferriate.	Nell'edificio sono installati degli estintori che vengono periodicamente revisionati secondo le disposizioni normative.	L'accesso all'edificio avviene tramite un portone usato per l'accesso del pubblico e due porte secondarie usate dalla Polizia Municipale e dai servizi Sociali. Le chiavi di accesso del comune sono state consegnate ai dipendenti ed agli amministratori
Biblioteca che si trova al primo piano dell'edificio	Le finestre del piano non sono protette con delle inferriate.	Nell'edificio sono installati degli estintori che vengono periodicamente revisionati secondo le disposizioni normative.	Alla biblioteca si accede tramite una porta in vetro alluminio che da su una rampa di scale che conduce al primo piano dell'edificio. L'accesso alla biblioteca avviene tramite una porta di Legno. Le chiavi delle porte sono state consegnate ai dipendenti che lavorano nel settore e alla banda del paese che utilizza un locale attiguo alla biblioteca.

9.6.2 Aree ad accesso non controllato

Sono quelle aree in cui il pubblico può accedere senza alcuna identificazione o misura di sicurezza (corridoi, sale per riunioni ecc).
In queste aree non devono essere installate apparecchiature informatiche contenenti dati personali; non devono essere presenti apparecchiature collegate alla rete del Comune di Ome se le stesse non sono presidiate da un operatore o protette da psw e spente se non sono presidiate.
Eventuali apparati di rete devono essere installati in armadi chiusi a chiave.
In questa categoria rientrano le sale di attesa e la sala consigliare ed i corridoi.
Attualmente queste questi locali rispettano le indicazioni di sicurezza definite.

9.6.3 Aree ad accesso controllato

Sono quelle aree in cui può accedere solamente il personale dipendente del Comune, nel caso in cui acceda del personale esterno questo deve essere identificato in un apposito registro o accompagnato da un collaboratore del Comune di Ome. In questa tipologia rientrano gli uffici comunali e anche gli sportelli accessibili al pubblico che durante l'orario di apertura devono essere presidiati dai collaboratori del Comune di Ome.
Queste aree/uffici al termine dell'orario di lavoro o di chiusura degli sportelli devono essere chiuse al pubblico.
In queste aree possono essere installate apparecchiatura informatiche collegate alla rete interna.
Le stazioni di lavoro devono rispettare una serie di misure minime di sicurezza:

- Accesso alle risorse del SI attraverso password conosciuta unicamente dall'operatore.
- Le sessioni di lavoro sono protette da un blocco dell'accesso al pc che entra in funzione dopo un determinato intervallo di tempo.
- Eventuali apparati di rete devono essere disposti in armadi chiusi.

9.6.4 Aree ad accesso ristretto

Sono quelle aree in cui sono installate apparecchiature critiche quali server, apparati di rete, L'accesso a tali aree è consentito solamente al personale addetto alla manutenzione del sistema informativo e al personale del comune.
Le aree ad accesso ristretto identificate presso il Comune di Ome sono essenzialmente:

- Ufficio in cui sono collocati i Server
- Archivi di deposito e storico del comune

Accesso da parte del personale esterno alla sala server

Il personale esterno (esclusi gli amministratori di sistema incaricati) che deve accedere agli uffici in cui sono installati i server del Comune di Ome per la manutenzione degli apparati, degli applicativi software o degli impianti, deve registrare l'attività svolta su un rapporto di intervento che verrà poi consegnato al responsabile dei sistemi informativi. Quando delle persone entrano nell'ufficio in cui sono collocati i server il loro operato è supervisionato da un collaboratore dell'ufficio, che si preoccupa anche di impartire indicazioni inerenti le regole di accesso ai locali.
Nella tabella sottostante sono identificate le misure di protezione degli uffici nei

quali sono presenti apparati critici del sistema informativo del Comune di Ome.
Di seguito viene fatta una descrizione dei sistemi di protezione attivi.

Identificazione	Ubicazione	Modalità Accesso	Impianto antincendio	Apparecchi per il Condizionamento
Ufficio in cui è installato il Server	Palazzo Municipale	Locale ad accesso libero	Estintore nelle vicinanze	si

9.6.4.1 Alimentazione Elettrica-UPS

Per la protezione da sbalzi di tensione o mancanza di energia elettrica, tutti i server sono collegati ad un UPS. Il sistema consente di alimentare le macchine rilevate alla data per circa 15 minuti. Nel caso di installazione di nuove apparecchiature, il limite minimo da non superare è di dieci minuti e questo deve essere valutato Dal Responsabile dei Sistemi Informativi.

Accesso agli archivi documentali

L'accesso agli archivi di deposito è consentito solo al personale autorizzato. Le chiavi di accesso all'archivio sono in dotazione all'ufficio della **Segreteria**. Il personale dipendente del comune che deve prelevare un documento lo chiede all'archivista incaricato. Una volta consultato il documento lo stesso viene riposto nell'archivio.

Presso i vari uffici sono presenti degli archivi classificati come archivio corrente al quale hanno accesso i soli dipendenti del settore.

9.7 Regole di autenticazione al sistema informativo comunale

In questo paragrafo vengono identificate le politiche per la gestione logica della sicurezza delle informazioni che interessano quindi l'accesso alle basi di dati attraverso gli apparati del sistema informativo e gli applicativi software.

9.7.1 Identificazione utenti

Ogni utente può accedere alla rete del sistema informativo attraverso un identificativo (user id) univoco e password. L'identificativo e la password sono personali.
L'assegnazione dei diritti di accesso alla rete informatica o alla base di dati viene fatta dal responsabile del sistema informativo.

9.7.2 Regole di autenticazione

La password è assegnata a ciascun utente in forma riservata. Allo stesso è consentito di variarla. La gestione della password prevede una serie di misure sotto riportate atte a rendere efficace l'utilizzo della stessa:

- Lunghezza minima 8 caratteri;
- Deve essere sostituita ogni 3 mesi;
- Non deve essere simile alla precedente;
- Non deve essere comunicata ai colleghi;

- Non deve essere annotata su supporti accessibili o leggibili;
- Non deve contenere termini facilmente riconducibili all'incaricato.

Come si evince dalle indicazioni sopra riportate la gestione delle password coinvolge anche gli utenti che devono quindi attenersi alle indicazioni contenute in questo piano della sicurezza.

Il sistema informativo prevede due livelli di autenticazione:

I° livello: Autenticazione per accesso alle risorse del sistema
Il Comune di Ome, utilizza i servizi di autenticazione del dominio di windows che prevedono la definizione della lunghezza minima delle password a 8 caratteri e l'utilizzo di una complessità nella definizione del codice di autenticazione. La policy di sicurezza impostata prevede che il codice identificativo scada automaticamente almeno ogni 3 mesi.

II° Livello Autenticazione applicativa.
Per quanto riguarda gli accessi agli **applicativi di gestione dei vari uffici** sono state fornite precise istruzioni ai collaboratori sulla necessità di variare la password secondo le regole sopra indicate. Inoltre, per quelle soluzioni la cui gestione viene fatta da enti esterni, si deve prevedere la comunicazione della stessa al custode delle password come evidenziato nella tabella di seguito riportata.

Gli utenti amministratori di sistema devono disporre di account diversi, e le regole di gestione delle password devono seguire quanto specificato nel paragrafo precedente.

9.7.3 Gestione delle Password

Il comune di Ome ha assegnato il servizio di manutenzione del sistema informativo ad un azienda esterna. La persona incaricata da quest'ultima attraverso opportune autorizzazioni è in grado di accedere ad un personal computer della rete comunale per effettuare operazioni di manutenzioni o per accedere alle banche dati memorizzate sullo stesso.
Quindi nel caso in cui il titolare debba accedere a delle informazioni, in assenza di un dipendente, l'utente "amministratore di rete" ha la possibilità di garantirne l'accesso. Per l'accessibilità alle banche dati degli applicativi di gestione, in ogni ufficio del comune vi è la presenza di più di un operatore e in ogni caso in assenza del personale, l'accesso può essere fatto dall'utente amministratore di sistema.
Per cui al custode delle password vengono consegnate unicamente i codici di autenticazione delle applicazioni o dei servizi applicativi relativi ad enti esterni che sono identificati nella tabella che segue.

Servizio Applicativo	Fornitore	Nome del software	Password	Comunicazione al custode delle password
Psw dell'utente Amministratore di Rete	----------	Windows 2003	8 caratteri variata ogni 3 mesi	si
Portale Regione	Regione	Portali della	8 caratteri	si

Lombardia	Lombardia	Regione Lombardia	variata ogni 3 mesi	
Banca dati Siatel	Ministero entrate	Siatel	8 caratteri variata ogni 3 mesi	si
Banca dati catastale	Agenzia del Territorio	Sister	8 caratteri variata ogni 6 mesi	si
Banca dati INA SAIA	Ministero Interno	Portale CNSD	8 caratteri variata ogni 6 mesi	si
Banca dati Sicra e sicraweb	Saga	Sicra Sicr@web	8 caratteri variata ogni 6 mesi	No

9.7.4 Revoca delle password e dei permessi di accesso

La gestione dell'assegnazione dei diritti di accesso viene pianificata dal Responsabile dei sistemi Informativi.

Se un dipendente viene assunto dall'ente, l'ufficio competente fa una comunicazione al Responsabile dei sistemi che provvede ad assegnarli un profilo di accesso al sistema informativo in funzione dell'incarico al trattamento dei dati.

Nel caso un collaboratore del Comune di Ome si dimetta, i diritti di accesso devono essere revocati attraverso una richiesta al Responsabile dei sistemi Informativi da parte dell'ufficio coinvolto. Id e password non possono essere associate ad un altro utente.

Nel caso in cui il collaboratore ricopra un incarico diverso deve essere fatta una comunicazione al responsabile del sistema informativo il quale provvede a modificare i permessi di accesso ai dati e alle risorse del sistema informativo.

La richiesta, deve essere fatta in forma scritta al Responsabile del Sistema Informativo da parte del responsabile dell'ufficio "cedente" e deve essere fatta una richiesta di attivazione all'accesso a determinate banche dati da parte del Responsabile dell'Ufficio ricevente.

Le user-id inutilizzate per più di 6 mesi saranno disattivate autonomamente dal Responsabile dei Sistemi Informativi.
Nel caso un'utente del Comune di Ome si assenti per un determinato periodo di tempo, l'utente Amministratore di Sistema è in grado di cancellare la password impostata dall'utente e di creare un nuovo id in modo da poter accedere alle risorse del PC.
In modo analogo l'utente Amministratore del sistema è in grado di creare degli utenti temporanei per accedere agli applicativi di business.
Per quegli applicativi e strumenti elettronici il cui accesso è consentito esclusivamente tramite credenziali di autenticazione, la cui gestione e variazione non è riconducibile all'ufficio informatico, la stessa deve essere comunicata al custode delle password ogni qualvolta viene cambiata. La custodia delle buste contenenti le credenziali di autenticazione viene fatta Dai responsabili di settore in cassaforte o in un cassetto con serratura. Se per motivi di accesso alle risorse del

sistema informativo vengono usate queste credenziali il responsabile dell'ufficio informatico avverte l'incaricato del trattamento.

9.7.5 Attività dell'Amministratore di Sistema

Come previsto dalla direttiva del garante il comune deve adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità, adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;
L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.
Allo stato attuale il comune di Ome ha identificato e nominato l'amministratore del sistema informativo. La registrazione dei log è demandata ai servizi dei sistemi operativi installati sul server e sui computer.

9.8 Gestione delle informazioni e dei dati

9.8.1 Ricezione dei documenti su supporto cartaceo

I documenti su supporto cartaceo possono arrivare all'Ente attraverso:

- il servizio postale o altri vettori(corrieri);
- la consegna diretta agli uffici, ai funzionari, o agli uffici utente abilitati presso l'Amministrazione al ricevimento della documentazione (ufficio protocollo);
- gli apparecchi fax

I documenti, esclusi quelli non soggetti a registrazione di protocollo, devono pervenire al protocollo per la loro registrazione. Quelli pervenuti via fax sono soggetti alle stesse regole di registrazione degli altri documenti cartacei; in presenza di un sistema informatico che ne consente l'acquisizione in formato elettronico (fax management) si applicano le procedure previste per la ricezione dei documenti informatici.

9.8.2 Ricezione dei documenti informatici

Posta elettronica Certificata
La ricezione dei documenti informatici è assicurata tramite una casella di posta elettronica certificata riservata a questa funzione e accessibile solo all'ufficio preposto alla registrazione di protocollo.
L'indirizzo della casella elettronica è pubblicato sul sito internet del comune.
Il responsabile del servizio provvede a renderlo pubblico e a trasmetterlo al CNIPA ai sensi dell'articolo 12, comma 2, lettera c del DPCM 3 1/ 10/2000.

Posta Elettronica
Gli utenti del sistema informativo comunale sono dotati di caselle di posta elettronica. L'accesso a questo sistema è protetto da una password di accesso al pc che ne garantisce la riservatezza dei messaggi e dei documenti trasmessi.

- La casella di posta, assegnata all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
- E' fatto divieto utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti la propria attività o funzione svolta per l'ente, salvo diversa ed esplicita autorizzazione.
- Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per il Comune, ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Responsabile di settore.
- Per la trasmissione di file all'interno del comune è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati, se di dimensioni consistenti si consiglia di utilizzare le directory di scambio presenti sui file server, notificando a mezzo mail al destinatario la disponibilità del file stesso.

9.8.3 Trasmissione dei documenti cartacei

In questo paragrafo vengono identificate le regole per la trasmissione dei documenti cartacei nell'ambito del Comune di Ome.
Le regole adottate dall'ente prevedono:

- Le comunicazioni in ingresso vengono protocollate dall'ufficio del protocollo, e i documenti classificati come riservati o contenenti dati sensibili vengono registrati e inoltrati in busta chiusa all'ufficio competente.
- Nel caso di comunicazioni verso l'esterno, la preparazione della corrispondenza è gestita dai singoli uffici. La trasmissione di documenti che contengono dati sensibili inerenti lo stato di salute prevede l'utilizzo della "**doppia busta**". Il documento contenente dati sensibili viene messo in una busta e accompagnato da una missiva con le indicazioni del destinatario senza riferimenti a dati classificati come sensibili.
- Per la trasmissione di documenti cartacei tra uffici del Comune, compresi lo smistamento della posta da parte del protocollo, si devono rispettare una serie di principi, in particolare quello di necessità e pertinenza: i dati possono circolare solo per ragioni di servizio e per la necessità dei singoli uffici. Inoltre la corrispondenza non deve passare indiscriminatamente da più persone evitando passaggi superflui. In particolare la trasmissione della posta contenente dati sensibili relativi allo stato di salute deve avvenire in busta chiusa, inoltre la corrispondenza che non può essere smistata deve essere custodita in armadi chiusi a chiave.

9.8.4 Trasmissione dati in forma digitale

Le reti sono un insieme di host tra di loro comunicanti. Le reti sono suddivise a seconda della dimensione. Si parla di rete LAN che copre una distanza ridotta solitamente all'interno di un edificio. Queste tipologie di reti servono per collegare uno o più server a dei client e a delle periferiche.
Si parla di WAN quando l'estensione della rete assume contorni geografici ampi e differisce dalla LAN, anche perché il controllo o la proprietà non è di un singolo ente.
Si parla poi di internet che è una rete di reti controllate da diverse società che supporta protocolli standard che consentono la comunicazione di utenti diversi. Le

caratteristiche di internet si possono riassumere in questi tre punti:

Dimensione indeterminata: non è realmente possibile stabilire quale sia la dimensione di internet, identificare quanti siano il numero degli utenti;

Eterogenea i sistemi che si connettono ad internet hanno caratteristiche diverse tra di loro;

Esposizione fisica e logica, dato che non esiste un controllo degli accessi globale qualsiasi persona può accedervi e grazie alla sua connettività può raggiungere qualsiasi risorsa della rete.

Questo fa capire quali siano i problemi e le minacce che possono derivare da internet. Le vulnerabilità che possono derivare dall'uso di questo sistema si possono identificare in una serie di aspetti:

Anonimato

Un malintenzionato può collegarsi ad internet e creare dei problemi ad un sistema che si trova a migliaia di km di distanza, stando dietro uno scudo elettronico. Infatti i sistemi di autenticazione tra i PC non è di tipo fisico come quello umano, ed inoltre un attacco può passare attraverso percorsi tortuosi usando centinai di host della rete.

Presenza di numero esteso di punti di attacco

Quando un file od un'informazione transitano da un Personal Computer ad un altro, prima di raggiungere il destinatario transitano attraverso numerosi punti della rete. Questo implica che ci si deve "fidare" dei criteri di protezione e delle policy di accesso degli apparati intermedi.

Complessità del sistema

Internet è un aggregato si hardware, software e sistemi operativi diversi. Ottenere una protezione affidabile risulta molto difficile in un sistema di questo tipo. Una rete può mettere in comunicazione due host con sistemi operativi diversi e questo può generare dei problemi sulla sicurezza.

9.8.5 Accesso agli Archivi documentali correnti

In ogni ufficio del Comune di Ome sono presenti degli archivi documentali contenuti in armadi che sono opportunamente custoditi in luoghi ad accesso regolamentato (uffici o armadi con porta chiudibile a chiave).
Se durante le ore di lavoro l'operatore deve accedere ai documenti cartacei contenenti dati personali o dati relativi alla gestione del Comune, gli stessi devono essere trattati con attenzione in modo da non pregiudicarne la privacy o la sottrazione indebita. Al termine della consultazione gli stessi devono essere riposti con cura negli armadi da cui sono stati prelevati. Al termine dell'orario di lavoro si deve provvedere a chiudere gli armadi o gli uffici.
I documenti contenenti dati **sensibili** devono essere custoditi in armadi chiusi a chiave.
Nel caso di armadi ubicati in luoghi accessibili al pubblico, questi devono essere chiusi a chiave in modo da garantire la privacy e la consistenza delle informazioni contenute.

Distruzione archivi documentali

Nel caso alcuni documenti contenenti dati personali, sensibili o dati classificati come importanti non siano più utili questi devono essere distrutti in modo da non risultare leggibili.

Le regole di distruzione degli archivi documentali devono tenere conto delle normative e delle direttive valide per la conservazione di atti e documenti definite dalle leggi di settore.
La gestione dei documenti cartacei compete ai responsabili del trattamento dei dati ognuno per le proprie competenze.

9.8.6 Gestione degli Archivi elettronici

I dati in formato elettronico sono custoditi su:
- dischi ottici
- supporti magnetici

I supporti che contengono dati personali o sensibili devono essere custoditi in un armadio o cassetto chiuso a chiave.
Al termine dei loro utilizzo, quando non è più necessaria la conservazione, i supporti devono essere distrutti o cancellati tramite formattazione da parte dell'incaricato previa autorizzazione del responsabile del trattamento dei dati competente.

9.9 Gestione della sicurezza informatica

Senza la pretesa di offrire una classificazione formale e completa, possiamo considerare gli attacchi come violazioni delle proprietà di sicurezza precedentemente enunciate. I tipi di attacchi possono essere dunque:
- intercettazioni (violano la proprietà di segretezza dell'informazione);
- alterazioni (violano il requisito di integrità);
- generazioni (violano i requisiti di autenticità e di non-ripudio);
- interruzioni (minacciano la disponibilità del sistema).

Nella tabella sono elencate le caratteristiche principali di ogni categoria di attacco, insieme ad alcuni esempi presi da contesti reali.

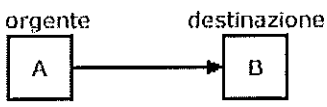
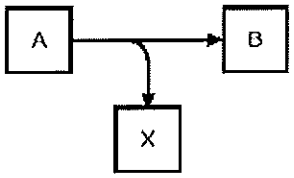
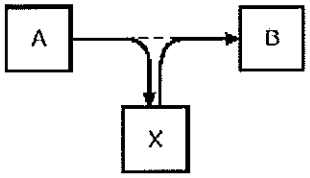
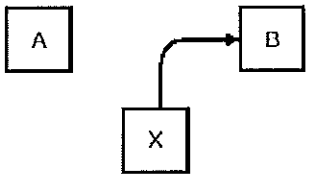
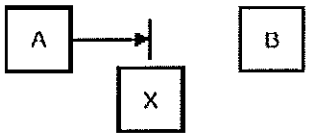
Attacco	*Schema*	*Esempi del mondo reale*
Flusso normale dell'informazione		Invio di un pacchetto IP Invio di email Accesso a una pagina web Lettura di dati da un database
Intercettazione		Sniffing di pacchetti di rete Furto di informazione mediante crittoanalisi Furto di informazione mediante analisi del traffico Furto di informazione mediante covert channel
Alterazione		Modifiche non autorizzate a file o programmi Attacchi man-in-the-middle Azioni di disturbo nel canale di comunicazione
Generazione		Masquerading Spoofing Intrusioni
Interruzione		Denial of service Flooding, resource starvation, mail storm Crashing di applicazioni Sabotaggio linee di comunicazione Danneggiamenti fisici

Tabella 1 – Le principali categorie di attacchi alla sicurezza informatica.

9.9.1 Sicurezza della rete

La rete consente alle varie stazioni di lavoro di collegarsi alle unità centrali di elaborazione dei dati. Una rete locale mediante opportuni apparati si può poi collegare ad internet, è intuitivo che i livelli di protezione del sistema informativo cambiano se si verifica quest'ultima condizione.

La rete del comune di Ome è configurata mediate la definizione di un dominio a cui accedono gruppi di utenti previa autenticazione. Per quanto riguarda la rete locale la politica di gestione degli indirizzamenti prevede l'utilizzo di uno schema di indirizzi IP che utilizzano il servizio DHCP.

9.9.2 Internet

Il rischio connesso al collegamento ad Internet della rete locale è quello di consentire a soggetti terzi di entrare ed operare nella LAN ed acquisire, modificare o distruggere risorse importanti come i dati in essa contenuti.
Il controllo della sicurezza viene mantenuto attraverso l'impostazione di una serie di misure minime volte a migliorare l'efficienza del sistema.
Uno degli strumenti attivati nel comune di Ome, per evitare che siano possibili

accessi indiscriminati ai dati privati, è costituito da **firewall**, attraverso il quale tutti i computer della rete accedono a Internet e viceversa, così che sia possibile impostare dei criteri per accettare o rifiutare le diverse connessioni.
L'apparato consente di effettuare un primo filtro e segnala in tempo reale attività relativi ad accessi sospetti. L'informazione di log consente di tracciare tutti gli accessi sospetti e di prendere le contromisure che il Responsabile dei Sistemi Informativi ritiene opportuno attuare.

9.9.3 Connessioni per Assistenza Remota

Il collegamento con le software house che devono connettersi al sistema informativo del comune per fare assistenza in modalità remota avviene utilizzando un tool per il controllo remoto e l'assistenza tecnica tramite internet. Attraverso questo tool è l'utente stesso che "cede" il controllo della propria macchina alla ditta che deve fare assistenza potendone osservare le attività che vengono fatte sulla stessa. Questa forma esplicita di collegamento da parte dell'utente permette un controllo sufficiente della sicurezza durante questa tipologia di attività. Al termine dell'intervento di assistenza il controllo remoto viene interrotto.

9.9.4 Virus informatici

I virus informatici sono dei programmi che possono causare dei guasti consistenti ai dati o ai programmi. I virus possono attaccare i file eseguibili e le macro contenute nei programmi di elaborazione dei dati. Molti virus possono essere introdotti nel sistema tramite pen-drive o collegandosi ad Internet. Una buona forma di difesa da questi attacchi consiste nel definire delle limitazioni al down load dei programmi ma anche un attento utilizzo delle potenzialità dei servizi offerti dal sistema informativo. A tale scopo è stato diffuso un decalogo contenente delle indicazioni sul buon uso delle risorse del sistema informativo, con lo scopo di sensibilizzare l'utente di fronte alle possibili tecniche di diffusione dei virus e quindi agli accorgimenti da attuare quando si presentano determinati eventi quali:

- messaggi di posta di cui non si conosce la provenienza
- messaggi di posta che contengono file eseguibili
- supporti magnetici da cui leggere determinati file ecc.
- accessi a siti di dubbia qualità

Altri elementi attuati per aumentare la sicurezza da virus sono:

- Limitare l'installazione di software che vengono scaricati da internet in modo che gli utenti non possano danneggiare l'efficienza e il funzionamento del sistema installando del sw di dubbia provenienza.
- Istruzione agli utenti al fine di controllare i supporti usati per lo scambio di dati o di file prima di utilizzarli

La responsabilità di verificare che l'aggiornamento dell'antivirus avvenga automaticamente è dell'utilizzatore dei personal computer, in caso contrario deve essere lanciato manualmente upgrade della suite antivirus.

9.9.5 Software antivirus

Il comune di Ome dispone di un sistema antivirus le cui caratteristiche di base sono di seguito elencate:

1. gli aggiornamenti devono essere resi disponibili non solo per posta ma anche tramite Internet;
2. deve essere particolarmente efficace contro i virus della nostra area geografica;
3. deve poter effettuare automaticamente una scansione ogni volta che viene avviato un programma;
4. deve poter effettuare una scansione automatica del Pen Drive;
5. deve accorgersi del tentativo di modificare le aree di sistema;
6. deve essere in grado di effettuare scansioni a intervalli regolari e programmati;
7. deve essere in grado di effettuare la scansione all'interno dei file compressi;
8. deve mantenere il livello di protezione in tempo-reale;
9. deve eseguire la scansione in tempo-reale;
10. deve poter eseguire la rimozione del codice virale in automatico;
11. in caso di impossibilità di rimozione i file non pulibili devono essere spostati una subdirectory
12. predefinita (quarantena);
13. deve essere in grado di effettuare la rilevazione/pulizia dei virus da Macro sconosciuti;
14. deve essere in grado di riconoscere i codici virali anche in file compattati utilizzando qualsiasi programma di compressione e in qualsiasi ambiente operativo.

Antivirus a bordo macchina (Client/Server)
Un sw antivirus è installato sui server del SI del comune e sui client. L'aggiornamento dell'antivirus avviene in modo automatico attraverso una procedura di update automatica.
Verifica del collegamento tra server su cui è installato l'antivirus e client della rete.
Script che aggiorna il client nel caso il sw installato abbia una versione superata.
Il prodotto è coperto da contratto di assistenza che annualmente viene rinnovato e che consente di aggiornare la suite con le nuove impronte virali messe a disposizione dal produttore.

I sw antivirus sono continuamente aggiornati attraverso la stipulazione di un contratto di assistenza con alla software house che lo produce.

9.10 Manutenzione del Sistema Informativo

In questo paragrafo vengono identificate le misure adottate dal Comune di Ome per la gestione delle apparecchiature, dei software applicativi e di sistema e per il mantenimento delle stessi in uno stato di efficienza.
La manutenzione è gestita da società specializzate e dalle aziende che hanno installato i software di gestione utilizzati dai vari uffici del comune.

9.10.1 Manutenzione dell'Hardware

Attualmente il server, i personal computer e le stampanti in dotazione presso il Comune di Ome nella sede municipale o negli uffici periferici, non sono coperti da contratto di manutenzione hardware.
I guasti agli apparati vengono affrontati di volta in volta facendo intervenire ditte specializzate.

9.10.2 Manutenzione Sistemistica

La manutenzione sistemistica del sistema informativo è affidata, su segnalazione degli utenti del sistema informativo, ad un'azienda esterna con la quale il comune ha sottoscritto un contratto di assistenza.
La società si occupa dell'installazione degli apparati di rete, degli apparti e dei tool di sicurezza, dei server, e dei PC; e gestisce gli aggiornamenti dei software di base.

9.10.3 Manutenzione Software

Annualmente il comune rinnova il contratto di assistenza software per gli applicativi gestionali usati dai vari uffici.

9.11 Criteri per il Ripristino della Disponibilità dei Dati

9.11.1 Copie dei Dati

I dati degli applicativi gestionali usati dai vari uffici del comune sono salvati sul server e copiati su un NAS giornalmente e conservate per 6 giorni diversi.
Oltre alle copie del server vengono fatte anche le copie su unità a nastro che vengono conservate in un luogo sicuro.

Le persone incaricate del backup fanno dei controlli attraverso un programma di verifica dell'esito del processo di copia.

Salvataggio		**Procedure di salvataggio**	**Ubicazione conservazione delle copie**	**Struttura incaricata del salvataggio**
Data Base	**Descrizione**			
Applicativo Segreteria	Sicr@web	Schedulata	Armadio chiuso a Chiave	Amministratore di Sistema
Applicativo Ragioneria	Sicra	Schedulata	Armadio chiuso a Chiave	Amministratore di Sistema
Applicativo Demografico	Sicra	Schedulata	Armadio chiuso a Chiave	Amministratore di Sistema
Gestione ICI	Sicra	Schedulata	Armadio chiuso a Chiave	Amministratore di Sistema
Gestione TARSU	Sicra	Schedulata	Armadio chiuso a Chiave	Amministratore di Sistema
Gestione Biblioteca	Sebina			
File di office	Cartelle Utenti	Schedulata	Armadio chiuso a Chiave	Amministratore di Sistema

9.11.2 Manutenzione dei supporti di backup

Il responsabile dei Sistemi Informativi ha il compito, di assicurare una costante

affidabilità ed efficacia delle operazioni di backup automatico e di provvedere alla manutenzione degli strumenti utilizzati.

9.11.3 Riutilizzo controllato dei PC

I PC dismessi vengono catalogati e conservati in un luogo chiudibile a chiave. Prima di essere dismessi si procede ad una formattazione del disco o alla distruzione die supporti di memorizzazione.

9.11.4 Disaster Recovery

L'implementazione di un piano della sicurezza, relativo ai sistemi informativi, deve tenere conto della necessità di ripristinare, in un determinato intervallo di tempo, le condizioni di funzionamento esistenti in seguito al verificarsi del guasto tecnico o di un attacco da parte di virus informatici. Il tempo di interruzione del servizio sopportabile dipende dalla criticità che riveste lo stesso ed in ogni caso non può superare i 7 giorni come previsto dal D Lgs 196/03. Il piano di continuità prevede le seguenti fasi:

La persona incaricata dei backup archivia i supporti removibili in un luogo sicuro. Presso l'ufficio del responsabile del sistema informativo sono custodite le copie, su supporto ottico, dei sistemi operativi e degli applicativi installati sui server e le istruzioni per il restore dei dati e delle configurazioni di sistema.
Nel caso di disastro che danneggia gravemente il sistema informativo del Comune di Ome il responsabile dei sistemi informativi attiva le società che si occupano della manutenzione sistemistica e della manutenzione degli applicativi gestionali.
Una volata predisposto l'hardware si procede al restore dei parametri di sistema, successivamente si installano gli applicativi software e si procede con il restore dei dati di business.
Questa operazione viene fatta utilizzando le copie di backup dei dati salvate sui server o le copie dei dati e le configurazioni salvate su supporti di backup.

Ripristino dei Dati		**Procedure di Ripristino**	**Struttura incaricata del Ripristino**
Data Base	**Descrizione**		
Applicativo Segreteria	Sicr@web	Standard	Ditte specializzate
Applicativo Ragioneria	Sicra	Standard	Ditte specializzate
Applicativo Demografico	Sicra	Standard	Ditte specializzate
Gestione ICI	Sicra	Standard	Ditte specializzate
Gestione TARSU	Sicra	Standard	Ditte specializzate
Gestione Biblioteca	Sebina		Provincia Brescia
File di office	Cartella Utenti	Standard	Ditte specializzate

10 Formazione

La gestione della sicurezza informatica in una qualsiasi organizzazione vede coinvolte in modo stretto gli utenti del sistema. Ciò richiede una costante formazione rivolta ad ogni dipendente che utilizza le risorse informatiche dell'organizzazione. L'obbiettivo è quello di creare la "cultura della sicurezza" attraverso una serie di attività volte ad illustrare i provvedimenti ed i comportamenti da adottare per migliorare la sicurezza informatica. Il piano è stato studiato, organizzato e predisposto sulla base delle specifiche esigenze di ciascuna area dell'ente in relazione alla natura dei dati trattati e dei rischi generici o specifici che incombono sui dati, nonché dei criteri e delle modalità di evitare tali rischi.

Il Comune di Ome ha fatto dei corsi di formazione per i dipendenti sulle tematiche inerenti la sicurezza dei sistemi informativi e relativi alla normativa sulla privacy.

10.1 Piano di formazione

Gli argomenti trattati nel corso di formazione sono essenzialmente i seguenti:

- informazioni sulla legge 196/2003 testo unico sulla Privacy;
- principi legislativi e comunitari;
- informazioni sulla normativa nell'ambito dei diritti del cittadino e comportamenti da adottare;
- soggetti interessati al trattamento dei dati
- misure minime di sicurezza;
- crimini informatici, frodi, abusi, danni, casistica;
- rischi possibili e probabili cui sono sottoposti i dati;
- misure di sicurezza tecniche ed organizzative e comportamentali deputate alla prevenzione dei rischi
- comportamenti e modalità di lavoro per prevenire i rischi di danneggiamento ai dati e alle risorse del sistema informativo.

11 Servizi affidati ad aziende/enti esterni

Il Comune di Ome affida ad alcuni fornitori/enti la gestione di alcuni servizi quali la manutenzione delle apparecchiature, degli applicativi software installati presso l'ente e servizi quali la gestione dell'assistenza domiciliare, l'erogazione dei pasti presso le scuole ecc. Questo implica che i collaboratori di queste aziende possano trattare parzialmente dati ed informazioni di cui il Comune di Ome è Titolare. A tale proposito il Comune di Ome ha nominato queste aziende responsabili del trattamento dei dati nell'ambito del loro operato.

12 Audit della Sicurezza

Le verifiche sulla corretta applicazione delle misure di sicurezza per la protezione dei dati e delle informazioni gestite dal Comune di Ome e delle misure particolari in riferimento esplicito a quelle previste dalla legge sul trattamento dei dati personali, sono affidate agli uffici di seguito identificati.

MISURE DA VERIFICARE	OGGETTO DELLE VERIFICHE	CADENZA	RESPONSABILE
Organizzazione			
Aggiornamento DPS	Controlli periodici, ed aggiornamento del DPS	Annua entro 31/3	Responsabile Segreteria
Outsourcing	Verifica criteri di sicurezza dei fornitori	a Campione	Settore che ha affidato all'esterno il servizio
Incarichi inerenti la sicurezza ed il trattamento dei dati	Controlli periodici degli incarichi, dei compiti e delle responsabilità.	Annua	Responsabile del servizio
Analisi dei rischi inerenti il sistema informativo e le banche dati	Analisi dei rischi e delle contromisure da adottare per contrastarli.	Annua	Amministratore del Sistema Informativo
Autorizzazioni all'accesso alle banche dati del sistema informativo	almeno una volta l'anno, è verificata la sussistenza delle condizioni per la loro conservazione	Annua	Amministratore del Sistema Informativo
Piano di formazione	Attivazione del piano di formazione per nuovi collaboratori del comune	Sempre	Segretario Comunale
Protezione fisica			
Protezione delle aree e dei locali	controlli periodici degli impianti e dei sistemi di sicurezza	Annua	Lavori e servizi pubblici, Manutenzioni
Antincendio	Manutenzione periodica	Secondo le indicazioni dell' installatore	Lavori e servizi pubblici, Manutenzioni
UPS	Manutenzione preventiva UPS Secondo le istruzioni del costruttore.	Secondo le indicazioni dell' installatore	Amministratore del Sistema Informativo
Controllo accessi fisici ai locali	controlli periodici dei sistemi che regolano l'accesso agli edifici, agli archivi o alle aree ad accesso ristretto.	continua	Lavori e servizi pubblici, Manutenzioni
Protezione Logica			
Criteri e procedure per assicurare	Controlli accessi banche dati.	Annua	Amministratore del Sistema Informativo

l'integrità dei dati	Controllo utilizzo modalità di autenticazione		
Codici identificativi personali	disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore	Sempre	Amministratore del Sistema Informativo
Restrizioni di accesso per via telematica	Controllo account sistema informativo	Annua	Amministratore del Sistema Informativo
Sicurezza delle trasmissioni dei dati	controlli periodici log dei firewall	periodica	Amministratore del Sistema Informativo
Sistema Informativo			
Antivirus	Verifica buon funzionamento Verifica aggiornamento	Annuale	Amministratore del Sistema Informativo
Patching	Aggiornamento periodico dei sistemi informativi dei server Aggiornamento periodico dei sistemi informativi dei client	Ogni mesi	Amministratore del Sistema Informativo
Back-up Dati	Verifica back-up dei dati e dei dati di sistema e efficienza apparecchiature e supporti.	Quotidiana	Amministratore del Sistema Informativo