Comune di Castel Baronia
Provincia di Avellino

Manuale di Gestione Documentale
(art. 5 DPCM 3/12/2013)
Allegato 1 - Piano di Sicurezza

Cod. **MANGEDOC** Rev. **1.0** Data: 20-07-2016

Sommario: In questo allegato viene riportato il Piano di sicurezza dei documenti informatici adottato dall'Ente.

REVISIONI

Rev.	Data	Redattore/i	Descrizione
1.0	20-07-2016	Maria Pia Papa	Prima stesura

INDICE

1 Premessa

Nel rispetto dell'approccio metodologico descritto nel capitolo 4 del Manuale di Gestione documentale il presente piano di sicurezza è strutturato nei seguenti argomenti:

- organizzazione dell'Ente ed organigramma di tutti i soggetti che provvedono al trattamento dei dati personali, con una descrizione dei ruoli, delle mansioni e delle responsabilità;
- censimento dei trattamenti di documenti con procedure informatiche e misure di sicurezza adottate;
- rilevazione dei luoghi fisici e delle misure di sicurezza già adottate dall'Ente;
- rilevazione del livello di informatizzazione dell'Ente e delle misure di sicurezza eventualmente adottate dall'Ente, svolto attraverso un accurato censimento delle risorse hw e sw utilizzate per la gestione documentale
- analisi dei rischi;
- valutazione delle possibili soluzioni adottabili per il raggiungimento dei livelli di sicurezza richiesti dal D.Lgs 196/03 e dal relativo allegato B (disciplinare tecnico).

2 Distribuzione di compiti e responsabilità

Nella procedura organizzativa "*Aree Organizzative Omogenee ed Organizzazione*" è riportato l'organigramma di tutti i soggetti che nell'ambito dell'Ente provvedono al trattamento dei documenti, con una descrizione di ruoli, mansioni e responsabilità.

In essa è anche specificato l'affidatario del ruolo di Amministratore del Sistema informativo comunale di Castel Baronia, in attuazione del punto c) del provvedimento del Garante del 27-11-2008 pubblicato in gazzetta ufficiale n. 300 del 24-12-2008 "Funzioni di amministrazione di sistema".

Nella procedura organizzativa "*Amministratori di Sistema*" si riportano informazioni sulle modalità con cui questo Ente amministra il Sistema Informativo e le funzioni affidate all'Amministratore stesso.

3 Censimento dei trattamenti dei documenti e aspetti di sicurezza correlati

La gestione di documenti digitali effettuati dall'Ente si articola nelle operazioni ampiamente descritte in questo Manuale che quì si elencano:

- Formazione
- Registrazione, classificazione e fascicolazione
- Archiviazione nel repository documentale
- Accesso ai documenti informatici e consultazione
- Trasmissione e interscambio
- Conservazione dei documenti informatici
    - *Servizio archivistico*
    - *Servizio di conservazione a norma*
    - *Conservazione dei documenti informatici e delle registrazioni di protocollo*
    - *Conservazione delle registrazioni di sicurezza*

In questo paragrafo vengono riesaminati, uno per volta, tutti i trattamenti sopra censiti evidenziando gli aspetti di sicurezza che li riguardano.

3.1 Formazione dei documenti

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e l'amministrazione/AOO di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO e tra AOO diverse.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o text editor e possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.

L'evolversi delle tecnologie e la crescente disponibilità e complessità dell'informazione digitale fa sì che non si possa definire in modo statico l'elenco di formati validi per la formazione dei documenti, pertanto occorre fare riferimento all'elenco dei formati pubblicati online sul sito dell'Agenzia per l'Italia digitale che viene periodicamente aggiornato sulla base dell'evoluzione tecnologica e dell'obsolescenza dei formati.

Nell'allegato "Formati dei documenti elettronici", è riportato l'elenco dei formati attualmente accettati da questo Ente.

I documenti informatici prodotti dall'AOO con prodotti di text editor sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF, XML e TIFF) come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.

Per attribuire una data certa a un documento informatico prodotto all'interno di una AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 (regole tecniche in materia di generazione e verifica delle firme elettroniche avanzate, qualificate e digitali …"). L'allegato "Sottoscrizione dei documenti informatici" descrive le regole per l'uso della firma elettronica e digitale all'interno dell'Ente e fornisce l'elenco dei documenti prodotti dall'Ente, soggetti o meno alla sottoscrizione con firma digitale.

L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza; i documenti così formati, prima di essere inviati a qualunque altra stazione di lavoro interna all'AOO, sono sottoposti ad un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'amministrazione/AOO.

3.2 Gestione dei documenti informatici

L'art. 7 del D.P.C.M. 03/12/2013 ha ripreso, aggiornandoli, i requisiti minimi di sicurezza che devono soddisfare i sistemi di protocollo informatico. Essi sono i seguenti: "

1. *il **sistema di protocollo informatico** assicura:*
   a. *l'univoca identificazione ed autenticazione degli utenti;*
   b. *la protezione delle informazioni relative a ciascun utente nei confronti degli altri;*
   c. *la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;*
   d. *la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione;*
2. *il sistema di protocollo informatico deve consentire il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti;*
3. *il sistema di protocollo informatico deve consentire il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore;*
4. *le registrazioni di cui ai commi 1, lettera d), e 3 devono essere protette da modifiche non autorizzate;*
5. *il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto;*
6. *il sistema di protocollo rispetta le misure di sicurezza previste dagli articoli da 31 a 36 e dal disciplinare tecnico di cui all'allegato B del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196."*

Le **registrazioni di sicurezza** sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) - presenti o transitate sul sistema informatico di protocollo - che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza sono costituite:

- dai log di sistema generati dal sistema operativo;
- dai log dei dispositivi di protezione periferica del sistema informatico [Intrusion Detection System (IDS), sensori di rete e firewall];
- dalle registrazioni del sistema informatico di protocollo.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal Servizio per la gestione documentale e dal titolare dei dati e, ove previsto, dalle forze dell'ordine.

3.3 Trasmissione e interscambio dei documenti informatici

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni

che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.

Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Il server di posta certificata del fornitore esterno (provider) di cui si avvale l'amministrazione, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

- accesso all'indice dei gestori di posta elettronica certificata allo scopo di verificare l'integrità del messaggio e del suo contenuto;
- tracciamento delle attività nel file di log della posta;
- gestione automatica delle ricevute di ritorno.

Lo scambio per via telematica di messaggi protocollati tra AOO di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal decreto legislativo del 30 giugno 2003, n. 196.

Per garantire alla AOO ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, viene utilizzata la tecnologia di firma digitale a disposizione delle amministrazioni coinvolte nello scambio dei messaggi.

All'esterno della AOO

La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dalla Circolare n. 60 del 23 gennaio 2013 che definisce il formato e la tipologia di informazioni minime ed accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni, opera una revisione della circolare AIPA/CR/28 del 7 maggio 2001 abrogandola e sostituendola a decorrere dalla conclusione dell'iter di emanazione dei decreti attuativi delle disposizioni del Codice dell'Amministrazione Digitale in materia di documento informatico e gestione documentale, protocollo informatico e di formazione e conservazione dei documenti informatici.

All'interno della AOO

Per i messaggi scambiati all'interno della AOO con la posta elettronica non sono previste ulteriori forme di protezione rispetto a quelle indicate nel piano di sicurezza relativo alle infrastrutture.

3.4 Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso (pubblica e privata) ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.

Nell'allegato "Abilitazioni all'utilizzo del sistema informatico di protocollo" esse vengono schematizzate.

Le relative politiche di composizione, di aggiornamento e, in generale, di sicurezza delle password sono riportate nell'Allegato "Politiche di sicurezza".

Il sistema informatico di protocollo adottato dall'Amministrazione/AOO:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente;
- assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Ciascun utente del sistema può accedere solamente ai documenti che sono stati assegnati alla propria unità organizzativa o agli uffici ad essa subordinati.

Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

Utenti interni alla AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal Responsabile del Servizio per la gestione documentale dell'Amministrazione/AOO. Tali livelli si distinguono in:

- abilitazione alla consultazione,
- abilitazione all'inserimento,
- abilitazione alla cancellazione
- abilitazione alla modifica delle informazioni.

Utenti esterni alla AOO – altre AOO/Amministrazioni

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione da parte di altre AOO avviene nel rispetto dei principi della cooperazione applicativa, secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui al decreto legislativo 28 febbraio 2005, n. 42.

Le AOO che accedono ai sistemi di gestione informatica dei documenti attraverso il SPC utilizzano funzioni di accesso per ottenere le seguenti informazioni:

- numero e data di registrazione di protocollo del documento inviato/ricevuto, oggetto, dati di classificazione, data di spedizione/ricezione ed eventuali altre informazioni aggiuntive opzionali;
- identificazione dell'ufficio di appartenenza del Responsabile del Procedimento.

Utenti esterni alla AOO - privati

Per l'esercizio del diritto di accesso ai documenti, sono possibili due alternative:

1. l'accesso diretto per via telematica
2. l'accesso attraverso l'Ufficio Relazioni con il Pubblico (URP).

L'accesso per via telematica da parte di utenti esterni all'amministrazione è consentito solo con strumenti tecnologici che permettono di identificare in modo certo il soggetto richiedente, quali: firme elettroniche, firme digitali, Carta Nazionale dei Servizi (CNS), Carta d'Identità Elettronica (CIE), sistemi di autenticazione riconosciuti dall'AOO.

L'accesso attraverso l'URP prevede che questo ufficio sia direttamente collegato con il sistema di protocollo informatico e di gestione documentale sulla base di apposite abilitazioni di sola consultazione concesse al personale addetto.

Se la consultazione avviene allo sportello, di fronte all'interessato, a tutela della riservatezza delle registrazioni di protocollo, l'addetto posiziona il video in modo da evitare la diffusione di informazioni di carattere personale.

Nei luoghi in cui è previsto l'accesso al pubblico e durante l'orario di ricevimento devono essere resi visibili, di volta in volta, soltanto dati o notizie che riguardino il soggetto interessato.

3.5 Conservazione dei documenti informatici

La conservazione dei documenti informatici avviene con le modalità e con le tecniche specificate nel D.P.C.M. 03/12/2013 "Regole tecniche per la conservazione" e nella Circolare dell'Agenzia per l'Italia Digitale n. 65 del 10 aprile 2014.

Servizio archivistico

Il responsabile del sistema archivistico dell'AOO ha individuato la sede dell'archivio dell'amministrazione già attiva per questa funzione.

Il responsabile del servizio in argomento ha effettuato la scelta a seguito della valutazione dei fattori di rischio che incombono sui documenti (ad es. rischi dovuti all'ambiente in cui si opera, rischi nelle attività di gestione, rischi dovuti a situazioni di emergenza).

Per contenere i danni conseguenti a situazioni di emergenza, il responsabile del servizio ha predisposto e reso noto, un piano individuando i soggetti incaricati di ciascuna fase.

Sono state pure regolamentate minutamente le modalità di consultazione, soprattutto interne, al fine di evitare accessi a personale non autorizzato.

Il responsabile del servizio di gestione archivistica è a conoscenza, in ogni momento, della collocazione del materiale archivistico e ha predisposto degli elenchi di consistenza del materiale che fa parte dell'archivio di deposito e un registro sul quale sono annotati i movimenti delle singole unità archivistiche.

Per il requisito di "accesso e consultazione", l'AOO garantisce la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti adottando i formati previsti dalle regole tecniche vigenti.

Servizio di conservazione sostitutiva

Il responsabile della conservazione sostitutiva dei documenti, operando d'intesa con i responsabili del trattamento dei dati personali, della sicurezza e dei sistemi informativi, provvede, tra l'altro alla

a) verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
b) adozione delle misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adozione di analoghe misure in riferimento all'obsolescenza dei formati;
c) duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
d) adozione delle misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art.12 DPCM 3/12/2013 (Regole tecniche in materia di conservazione).

4 Il sistema informatico di supporto alla gestione documentale

Durante l'intervento nella/e sede/i dell'Ente è stato visionato il sistema informativo attraverso le sue componenti hardware e software e sono state rilevate le misure di sicurezza intraprese dall'Ente su tali risorse.

Il RSP ha adottato le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni:

- protezione periferica della Intranet dell'amministrazione/AOO;
- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza trimestrale durante la fase di esercizio;
- piano di continuità del servizio con particolare riferimento sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;
- conservazione, a cura dei servizi informatici delle copie di riserva dei dati e dei documenti, in locali diversi e se possibile lontani da quelli in cui è installato il sistema di elaborazione di esercizio che ospita il Sistema di Protocollo Informatico;
- gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne qualificate (o ricorrendo a strutture esterne qualificate);
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- cifratura o uso di codici identificativi (o altre soluzioni ad es. separazione della parte anagrafica da quella "sensibile") dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, allo scopo di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità;
- impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati idonee a rilevare lo stato di salute e la vita sessuale;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema.

5 Analisi dei rischi

5.1 Fattori di rischio per la sicurezza

L'analisi dei rischi è uno dei più importanti elementi per inquadrare i rischi ed individuare le appropriate misure di sicurezza[1].

I rischi che vengono presi in considerazione sono di due tipi, a seconda che riguardino il rispetto delle imposizioni del codice della privacy, oppure il più vasto mondo dei rischi propri di un sistema informativo.

La differenza tra le due categorie di rischi è fondamentale, perché mentre nella seconda categoria sono compresi tutti i rischi della prima, nella prima categoria sono contemplati solo quei rischi, direttamente afferenti alla tutela dei dati personali.

In altri termini, se un sistema informativo che gestisce servizi al pubblico si arresta alle ore 10 del mattino di un giorno feriale, per mancanza di energia al server centrale, i clienti diventano impazienti, gli operatori di sportello tempestano di telefonate il centro elettronico, la direzione viene inondata di proteste, ma le disposizioni del codice sulla protezione dei dati personali non vengono violate, perché siamo ancora ben lontani dai tempi di ripristino del servizio di trattamento, indicati dal codice stesso.

Si vede subito che la differenza fra le misure minime e le misure necessarie non è quindi solo legata allo stato dell'arte delle misure, ma anche alle misure stesse che possono garantire da certi rischi ritenuti molto grandi, ma di cui la legge ignora l'esistenza perché non afferenti alla protezione di dati personali.

L'analisi di rischio sarà quindi volta ad identificare, valutare e contrastare

- i rischi propri indicati dalla legge, e cioè il rischio di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- i rischi individuati nella gestione del sistema informativo.

Alla prima categoria si bada per obbligo di legge; alla seconda categoria occorre badare per garantire il regolare svolgimento dell'attività esercitata e la continuità dei servizi ai cittadini.

Più l'analisi dei rischi viene fatta accuratamente, anche per rischi non legati specificatamente al trattamento di dati personali, più questo allegato rappresenta in modo esauriente e completo il manuale per la sicurezza del sistema informativo, che include tutte le misure atte a tutelare la privacy, ma che comprende anche tutte le misure rilevantissime per la sopravvivenza dell'Ente stesso.

Nell'analisi di impatto che segue si prendono in considerazione le seguenti macro-categorie di rischi, connesse all'utilizzo di sistemi di elaborazione, che possono generare danni e che comportano quindi rischi per la sicurezza dei dati:

- ***Uso non autorizzato dell'Hardware (Unah)***

[1] Il modello di analisi dei rischi proposto in questo capitolo è stato elaborato sulla base di principi utilizzati nel campo del risk management tipici dell'ingegneria del software e applicato, con i dovuti adattamenti, al settore della sicurezza. Il modello è stato, poi, sperimentato in alcune decine di Enti Locali in occasione dell'adeguamento al D.Lgs. 196/2003, per la messa in sicurezza dei sistemi informativi e per la protezione dei dati personali trattati.

- ***Rivelazione illegittima di informazioni, anche per negligenza (Riin)***
- ***Alterazione non autorizzata di informazioni (Anai)***
- ***Perdita di informazioni (Prin)***
- ***Uso non autorizzato di informazioni (Unai)***
- ***Uso non autorizzato di applicativi (Unaa)***
- ***Perdita o riutilizzo di supporti cartacei o magnetici o documentazioni accessorie (Psup)***

e si valuta l'impatto sulla sicurezza che ha ognuna delle macro-categorie di rischio suddette.

Quindi, per ognuna delle macrocategorie di rischio individuate, si esamina un ulteriore e più dettagliato ventaglio di **fattori di rischio** che risultano critici per la sicurezza dei dati trattati nell'Ente.

Nella tabella seguente si riportano i fattori di rischio individuati:

Fattori di Rischio	Descrizione dell'impatto sulla sicurezza
Furto di credenziali di autenticazione per l'accesso ad un computer	Permette all'intruso di poter accedere ad una stazione di lavoro o ad un server con le autorizzazioni legate alle credenziali sottratte e arrecare qualsiasi tipo di danno ai dati trattati.
Utilizzo potenza di calcolo a propri fini	In questo contesto si inquadra il trattamento non consentito o non conforme di dati personali (violazione dell'art. 167 - illecito penale).
Azione di virus informatici o di codici malefici	Tali programmi potrebbero alterare il funzionamento delle applicazioni software. L'azione dei programmi non conosciuti o nascosti è tra le forme più insidiose di danneggiamento che possono essere arrecate agli strumenti elettronici.
Spamming o altre tecniche di sabotaggio	Tutte le forme di ingolfamento dei sistemi elettronici e quelle di sabotaggio sono soggette alle azioni previste dal codice civile e penale.
Furto di credenziali di autenticazione per l'accesso alle applicazioni software censite	Permette all'intruso di poter accedere alla specifica applicazione software con le dovute autorizzazioni legate a quelle credenziali sottratte e arrecare qualsiasi tipo di danno sui dati trattati.
Accesso non autorizzato a informazioni e dati presenti nelle applicazioni software censite	Permette ad utenti autenticati del Sistema Informativo di accedere ad informazioni senza la necessaria autorizzazione ovvero di accedere ad informazioni per le quali non è possibile predisporre un profilo di autorizzazione informatica.
Malfunzionamento, indisponibilità o degrado degli strumenti	Per prevenire situazioni di malfunzionamento hw/sw il Comune deve disporre di contratti di assistenza e manutenzione attivi che permettano il controllo e monitoraggio dell'attività dei sistemi; inoltre è necessario adottare opportune misure di sicurezza al fine di garantire il ripristino dei dati e delle applicazioni software in caso di distruzione degli strumenti.
Guasto tecnologico ai sistemi complementari (impianto elettrico,	Anche in questi casi è necessario adottare opportune misure di sicurezza al fine di prevenire danni (sistemi di allarme, ...) e, in caso di distruzione degli strumenti, garantire il ripristino dei dati e

Fattori di Rischio	Descrizione dell'impatto sulla sicurezza
climatizzazione, ...)	delle applicazioni software.
Carenza di consapevolezza, disattenzione o incuria	Questo atteggiamento può provocare i maggiori danni su ciascun trattamento da parte dell'incaricato.
Errori umani nella gestione della sicurezza	E' sempre possibile commettere errori nell'adoperare gli strumenti elettronici. Quando viene effettuato un trattamento su dati personali l'incaricato dovrà attenersi alle regole di verifica sull'esattezza delle informazioni trattate. E' necessario impartire le dovute istruzioni agli operatori che trattano direttamente o indirettamente con gli strumenti elettronici.
Comportamenti sleali o fraudolenti	Il trattamento illecito dei dati è soggetto alle sanzioni previste dal codice penale. L'incaricato dovrebbe essere consapevole che il trattamento dei dati personali è soggetto alla tutela così come previsto dal codice D.lgs. 196/2003, dal codice civile (art. 2050) e dagli specifici articoli del codice penale.
Accessi esterni non autorizzati	La regolamentazione degli accessi ai locali del Comune è un aspetto delicato che va affrontato attraverso regole e autorizzazioni a tutti i livelli.
Intercettazione di informazioni in rete	E' necessario, per i sistemi collegati alla rete Internet e intranet, dotarsi di dispositivi che permettano il monitoraggio della rete telematica per consentire l'attuazione di opportune misure di sicurezza a favore del buon funzionamento dei sistemi informativi.
Accessi non autorizzati a locali/reparti ad accesso ristretto	I locali adibiti ad ospitare sistemi e strumenti per il trattamento elettronico dei dati personali vanno protetti da tutti i possibili pericoli per intrusioni o accessi non consentiti.
Asportazione e furto di strumenti contenenti dati	I dispositivi di memorizzazione dei dati devono essere collocati in luoghi sicuri e protetti.
Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	In qualsiasi momento i sistemi sono esposti a queste forme di rischio. E' necessario adottare opportune misure di sicurezza al fine di prevenire danni agli strumenti elettronici e garantire, in caso di distruzione, il ripristino dei dati e delle applicazioni in essi contenuti.

L'analisi dei rischi, fatta nel paragrafo 5.3, evidenzia, per ciascuno dei fattori di rischio individuati, il livello di criticità, ovvero il livello di difficoltà da parte dell'Ente di garantire il non accadimento dell'evento dannoso.

5.2 Analisi d'impatto

L'obiettivo di sicurezza è ottenuto in particolare mediante il perseguimento di appropriate misure di sicurezza.

In questo paragrafo viene valutato l'impatto delle macro-categorie di rischio individuate rispetto alla sicurezza dell'Ente; la valutazione viene fatta su una scala che prevede quattro valori qualitativi:

0 = impatto basso

1 = impatto medio

2 = impatto alto; aspetto importante

3 = impatto molto alto; aspetto fondamentale

La valutazione è utilizzata nel seguito del documento per orientare le scelte sulle politiche di sicurezza da adottare.

Le tabelle seguenti sintetizzano i profili delle categorie di rischio specificando, per ogni macrocategoria, l'impatto che quest'ultima ha sulla sicurezza dell'Ente, secondo la scala definita precedentemente.

Per ogni macro-categoria, viene marcata con una X la misura dell'impatto.

Per ogni macro-categoria, viene aggiunta sempre una adeguata spiegazione che motivi la misura dell'impatto individuata.

Acr	Macro-categoria di rischio	Impatto				Motivazione
		0	1	2	3	
Unah	**Uso non autorizzato dell'hardware** In molti casi i dipendenti possono utilizzare la potenza di calcolo della CPU per propri fini, magari archiviando in memoria dei programmi che vengono richiamati in servizio quando il controllo è meno stretto. La frequenza dei controlli e l'esame dei log di sistema sono determinanti nel rivelare questo tipo di perdite.			X		In questo contesto si inquadra il trattamento non consentito o non conforme di dati personali (violazione dell'art. 167 - illecito penale).
Riin	**Rivelazione illegittima di informazioni anche per negligenza** Il trattamento illecito dei dati è soggetto alle sanzioni previste dal codice penale. L'incaricato dovrebbe essere consapevole che il trattamento dei dati personali è soggetto alla tutela così come previsto dal codice D.lgs. 196/2003, dal codice civile (art. 2050) e dagli specifici articoli del codice penale				X	La rivelazione di informazioni può avere riflessi di triplice natura: penali, finanziari (connessi all'applicazione di sanzioni e risarcimenti), riflessi d'immagine. In Italia, grazie all'entrata in vigore della legge 675/96 e del presente codice, i riflessi che un tempo erano solo civili assumono rilevanza penale, il che significa che non sono sempre monetizzabili.
Anai	**Alterazione non autorizzata di informazioni** Un dipendente od un esterno possono alterare deliberatamente uno o più file del sistema di elaborazione. L'alterazione può avvenire tramite l'accesso ai sistemi per furto di credenziali di autenticazione, l'azione di virus e di codici malefici, lo spamming ed altre tecniche di sabotaggio			X		In questo caso il costo del risarcimento è legato al costo del ricontrollo di tutti i file potenzialmente affetti e non solo da quello eventualmente identificato. Si applicano inoltre sanzioni penali. Il ricontrollo viene fatto, tipicamente, per confronto con i dati cartacei originali, ammesso che essi siano ancora disponibili.
Prin	**Perdita di informazioni** Questa perdita può essere causata da eventi naturali o da atti dolosi o da errori od omissioni.				X	Il risultato finale, in termini di perdita, evidentemente non cambia, anche perché spesso è praticamente impossibile ricostruire con certezza la causa che ha generato una perdita di informazioni. Il costo della perdita è valutabile sulla base dei costi medi di ricostruzione dei dati, in termini di manodopera, di tempo macchina, di attrezzature. Restano impregiudicate le sanzioni penali.
Unai	**Uso non autorizzato di informazioni** Questo sinistro può appartenere ad una delle categorie già esaminate, se non fosse per il ruolo attivo e prolungato del perpetratore. Esso può avvenire in seguito a furto delle credenziali di autenticazione			X		Permette all'intruso di poter accedere ad una stazione di lavoro o ad un server con le autorizzazioni legate alle credenziali sottratte e arrecare qualsiasi tipo di danno ai dati trattati
Unaa	**Uso non autorizzato di applicativi** Permette ad utenti autenticati sul Sistema Informativo di accedere ad informazioni e dati gestite dalle applicazioni, senza la necessità			X		Il costo di questo sinistro è difficile da quantizzare e può perfino avere dimensioni tali da portare in fallimento l'Ente; tutto dipende dal tipo di applicativo coinvolto (standard oppure un raffinato

	di necessaria autorizzazione					programma di gestione). Se si tratta di applicazioni standard, il costo è assimilabile al costo di un utilizzo legittimo dell'applicazione; a tali costi vanno aggiunte le sanzioni penali, ove il trattamento non autorizzato abbia portato a violazioni della legge ed abbia ecceduto i limiti del consenso al trattamento, espresso dall'interessato.
Psup	**Perdita o riutilizzo di supporti cartacei o magnetici o documentazioni accessorie** In questa categoria si possono includere i supporti magnetici non cancellati, i libri o la documentazione di supporto, i manuali, i nastri per stampante, cassette video, altre attrezzature normalmente utilizzate nei centri EDP, parti di ricambio, strumenti. Restano impregiudicate le sanzioni penali, previste dal regolamento. La perdita o il riutilizzo improprio possono essere causati da atti deliberati (furti), accidentali, negligenza (disordine).			X		In seguito ad un evento di questo tipo, persone estranee possono venire a conoscenza di di dati personali e sensibili presenti sui supporti per cui il danno potrebbe assumere rilevanza molto alta.

5.3 Analisi dei rischi

La tabella seguente sintetizza, per ognuna delle macrocategorie di rischio definite precedentemente, i fattori di rischio che possono risultare critici per la sicurezza dei dati trattati dall'Ente, evidenziando per ciascuno di essi il livello di criticità, ovvero la difficoltà da parte dell'Ente stesso di garantire il non accadimento dell'evento dannoso (la scala di rilevanza è quella a quattro livelli già illustrata):

0 = criticità bassa
1 = criticità media
2 = criticità alta; aspetto importante
3 = criticità molto alta; aspetto fondamentale

I fattori di rischio evidenziati costituiscono il riferimento principale per la definizione di opportune contromisure da adottare che consentano di governare le criticità e di garantire la messa in sicurezza dell'Ente.

Nella colonna "Impatto" viene riportato dal paragrafo precedente l'impatto che ha ciascuna macro-categoria di rischio sulla sicurezza dell'Ente.

Accanto ad ogni fattore di rischio viene marcata con una X la sua criticità nella scala di rilevanza a quattro livelli, motivata adeguatamente.

Acr	Macro-categorie di rischio e fattori di rischio	Impatto				Criticità rilevate nel Comune				
		0	1	2	3	0	1	2	3	Motivazione
Unah	**Uso non autorizzato dell'Hardware**			X						
	Utilizzo potenza di calcolo a propri fini					X				Rischio non elevato nell'Ente

	Furto di credenziali di autenticazione			X			L'utilizzo delle credenziali di accesso (ID e Password) è strettamente riservato agli incaricati del trattamento. E' sempre meno frequente l'utilizzo da parte di più utenti delle medesime credenziali di accesso per accedere alle applicazioni software rilevate. La loro custodia deve essere garantita dai responsabili dei singoli servizi. Occorre regolamentare la procedura di gestione delle credenziali di autenticazione.
	Intercettazione di informazioni in rete		X				Le applicazione sw utilizzate e le rispettive banche dati sono meno esposte ad eventuali accessi dalla rete e relative intercettazioni, perché il Comune ha provveduto al collegamento in rete delle stazioni di lavoro degli incaricati ed alla messa in protezione della rete, anche tramite firewall; in tal modo la rete dati interna (LAN) è separata dal mondo esterno (WAN). Stabilire le regole di sicurezza per l'uso della posta elettronica ed internet e formare il personale.
	Valore Medio		**X**				
Riin	**Rivelazione illegittima di informazioni, anche per negligenza**				**X**		
	Comportamenti sleali o fraudolenti		X				Rischio non elevato nell'Ente. In qualche caso gli incaricati del trattamento potrebbero non essere consapevoli della gravità di tali azioni. L'Amministrazione comunale programma attività di aggiornamento periodico del personale incaricato ai trattamenti.
	Carenza di consapevolezza, disattenzione ed incuria	X					Un atteggiamento negligente, disattento ed inconsapevole può provocare i maggiori danni su ciascun trattamento da parte degli incaricati, non è molto diffuso nell'Ente.
	Intercettazione di informazioni in rete		X				Le applicazione sw utilizzate e le rispettive banche dati sono meno esposte ad eventuali accessi dalla rete e relative intercettazioni, perché il Comune ha provveduto al collegamento in rete delle stazioni di lavoro degli incaricati ed alla messa in protezione della rete, anche tramite firewall; in tal modo la rete dati interna (LAN) è separata dal mondo esterno (WAN). Stabilire le regole di sicurezza per l'uso della posta elettronica ed internet e formare il personale.
	Valore Medio		**X**				
Anai	**Alterazione non autorizzata di informazioni**				**X**		
	Furto di credenziali di autenticazione			X			L'utilizzo delle credenziali di accesso (ID e Password) è strettamente riservato agli incaricati del trattamento. E' sempre meno frequente l'utilizzo da parte di più utenti delle medesime credenziali di accesso per accedere alle applicazioni software rilevate. La loro custodia deve essere garantita dai responsabili dei singoli servizi. Occorre regolamentare la procedura di gestione delle credenziali di autenticazione.
	Azioni di virus informatici o codici malefici			X			Dalla rilevazione fatta, si evince che le postazioni di lavoro sono adeguate a fronteggiare tale rischio. E' garantita l'operazione di aggiornamento dei virus su tutte le postazioni di lavoro. Il Comune ha collegato in rete locale tutti i PC ed ha installato un antivirus centralizzato sul server che aggiorna quotidianamente tutte le postazioni di lavoro del Comune. Non abbassare la guardia.
	Spamming o altre tecniche di sabotaggio		X				Il Comune ha attivato il servizio di posta elettronica per la maggior parte degli uffici e la PEC per i Responsabili di struttura. Il servizio antispamming è fornito dai provider e dal firewall.

	Errori umani			X		E' sempre possibile commettere errori di digitazione sui dispositivi di input degli strumenti informatici. Devono essere impartite istruzioni agli operatori sulla necessità di verificare sempre l'esattezza dei dati impostati.
	Comportamenti sleali o fraudolenti		X			Rischio non elevato nell'Ente. In qualche caso gli incaricati del trattamento potrebbero non essere consapevoli della gravità di tali azioni. L'Amministrazione comunale programma attività di aggiornamento periodico del personale incaricato ai trattamenti.
	Accessi esterni non autorizzati		X			L'Ente è al riparo da accessi esterni non autorizzati di tipo fisico, avendo istituito nella sede principale il controllo degli accessi tramite uscieri. Si potrebbe istituire un registro degli accessi. Il Comune ha sostituito le serrature delle porte degli uffici che trattano dati sensibili con serrature a norma europea. Per quanto riguarda le misure di protezione di tipo logico è stato configurato un firewall per la protezione della rete LAN e l'antivirus su tutte le macchine.
	Carenza di consapevolezza, disattenzione o incuria			X		Un atteggiamento negligente, disattento ed inconsapevole può provocare danni notevoli. Il Comune deve porre particolare attenzione ad un piano programmato di back-up e recovery riguardante le banche dati delle principali applicazioni informatiche, così da poter ripristinare i dati in caso di alterazione.
	Valore Medio			**X**		
Prin	**Perdita di informazioni**				**X**	
	Azioni di virus informatici o codici malefici			X		Dalla rilevazione fatta, si evince che le postazioni di lavoro sono adeguate a fronteggiare tale rischio. E' garantita l'operazione di aggiornamento dei virus su tutte le postazioni di lavoro. Il Comune ha collegato in rete locale tutti i PC ed ha installato un antivirus centralizzato sul server che aggiorna quotidianamente tutte le postazioni di lavoro del Comune. Non abbassare la guardia.
	Spamming o altre tecniche di sabotaggio		X			Il Comune ha attivato il servizio di posta elettronica per la maggior parte degli uffici e la PEC per i Responsabili di struttura. Il servizio antispamming è fornito dai provider e dal firewall.
	Malfunzionamento, indisponibilità o degrado degli strumenti			X		L'Ente ha attivato un piano di adeguamento per mettersi al riparo da questi rischi tramite l'installazione di gruppi di continuità, azioni programmate di back-up e recovery configurate e tenute sotto controllo da un amministratore informatico. Non è stato attuato il Piano di Disaster & Recovery e Continuità Operativa approvato dalla ex DigitPA.
	Guasto tecnologico ai sistemi complementari			X		Non sono utilizzati impianti di condizionamento; solo in parte sono utilizzati gruppi di continuità; il sistema elettrico e di collegamento non è canalizzato e differenziato, quindi un corto circuito potrebbe innescare incendi. Esiste un impianto antincendio ed i computer sono sollevati da terra, quindi sono protetti da rischio di allagamento. Non è stato attuato il Piano di Disaster & Recovery e Continuità Operativa approvato dalla ex DigitPA.
	Carenza di consapevolezza, disattenzione o incuria		X			Un atteggiamento negligente, disattento ed inconsapevole può provocare danni notevoli. Il Comune ha posto, negli ultimi tempi particolare attenzione ad un piano programmato di back-up e recovery riguardante le banche dati delle principali applicazioni informatiche, così da per poter ripristinare i dati in caso di alterazione.
	Errori umani		X			E' sempre possibile commettere errori di digitazione sui dispositivi di input degli strumenti informatici. E' necessario impartire le dovute istruzioni agli operatori che trattano direttamente o indirettamente con gli strumenti elettronici.

	Asportazione e furto di strumenti contenenti dati		X			L'accesso ai locali è controllato, le porte e i balconi maggiormente accessibili, perché a piano terra, sono dotati di inferriate. E' stato istituito un luogo sicuro dove conservare i supporti di back-up relativi alle banche dati delle applicazioni sw gestite.
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria			X		Il Comune ha installato e mantiene un impianto antincendio; ha provveduto a sollevare i PC da terra contro il rischio di allagamento. Occorre fronteggiare ulteriormente il rischio attuando il Piano di Disaster & Recovery e Continuità Operativa.
	Valore Medio			**X**		
Unai	**Uso non autorizzato di informazioni**			**X**		
	Furto di credenziali di autenticazione per l'accesso ad un computer e/o alle applicazioni censite			X		L'utilizzo delle credenziali di accesso (ID e Password) è strettamente riservato agli incaricati del trattamento. E' sempre meno frequente l'utilizzo da parte di più utenti delle medesime credenziali di accesso per accedere alle applicazioni software rilevate. La loro custodia deve essere garantita dai responsabili dei singoli servizi. Occorre regolamentare la procedura di gestione delle credenziali di autenticazione.
	Comportamenti sleali o fraudolenti	X				In qualche caso gli incaricati del trattamento potrebbero non essere consapevoli della gravità di tali azioni. L'Amministrazione comunale programma attività di aggiornamento periodico del personale incaricato ai trattamenti. Non abbassare la guardia
	Accessi esterni non autorizzati		X			L'Ente è parzialmente al riparo da accessi esterni non autorizzati di tipo fisico, avendo istituito nella sede principale il controllo degli accessi tramite uscieri. Occorre dare istruzioni precise al guardiano fisso all'ingresso; si potrebbe istituire un registro degli accessi. Il Comune ha sostituito le serrature delle porte di uffici che trattano dati sensibili con serrature a norma europea. Per quanto riguarda le misure di protezione di tipo logico è stato configurato un firewall per la protezione della rete LAN.
	Intercettazione di informazioni in rete		X			Le applicazione sw utilizzate e le rispettive banche dati sono meno esposte ad eventuali accessi dalla rete e relative intercettazioni, perché il Comune ha provveduto al collegamento in rete delle stazioni di lavoro degli incaricati ed alla messa in protezione della rete, anche tramite firewall; in tal modo la rete dati interna (LAN) è separata dal mondo esterno (WAN). Stabilire le regole di sicurezza per l'uso della posta elettronica ed internet e formare il personale.
	Valore Medio		**X**			
Unaa	**Uso non autorizzato di applicativi**			**X**		
	Furto di credenziali di autenticazione per l'accesso alle applicazioni censite			X		L'utilizzo delle credenziali di accesso (ID e Password) è strettamente riservato agli incaricati del trattamento. E' sempre meno frequente l'utilizzo da parte di più utenti delle medesime credenziali di accesso per accedere alle applicazioni software rilevate. La loro custodia deve essere garantita dai responsabili dei singoli servizi. Occorre regolamentare la procedura di gestione delle credenziali di autenticazione.
	Comportamenti sleali o fraudolenti		X			In qualche caso gli incaricati del trattamento potrebbero non essere consapevoli della gravità di tali azioni. L'Amministrazione comunale programma attività di aggiornamento periodico del personale incaricato ai trattamenti. Non abbassare la guardia

	Accessi esterni non autorizzati			X			L'Ente è parzialmente al riparo da accessi esterni non autorizzati di tipo fisico, avendo istituito nella sede principale il controllo degli accessi tramite uscieri; nella sede destinata ai Servizi Sociali il portone d'ingresso viene tenuto chiuso ed è necessario bussare per potervi accedere. Occorre dare istruzioni precise al guardiano fisso all'ingresso; si potrebbe istituire un registro degli accessi. Il Comune ha sostituito le serrature delle porte di uffici che trattano dati sensibili con serrature a norma europea. Per quanto riguarda le misure di protezione di tipo logico è stato configurato un proxy server Linux per la protezione della rete LAN.
	Valore Medio			**X**			
Psup	**Perdita o riutilizzo di supporti cartacei o magnetici o documentazioni accessorie**			**X**			
	Malfunzionamento, indisponibilità o degrado degli strumenti				X		L'Ente ha attivato un piano di adeguamento per mettersi al riparo da questi rischi tramite l'installazione di gruppi di continuità, azioni programmate di back-up e recovery configurate e tenute sotto controllo da un amministratore informatico. Non è stato attuato il Piano di Disaster & Recovery e Continuità Operativa approvato dalla ex DigitPA.
	Carenza di consapevolezza, disattenzione o incuria	X					E' presente nell'Ente un atteggiamento consapevole sulle regole di mantenimento dei supporti magnetici ed ottici.
	Asportazione e furto di strumenti contenenti dati			X			L'accesso ai locali è controllato, le porte e i balconi maggiormente accessibili, perché a piano terra, sono dotati di inferriate. E' stato istituito un luogo sicuro dove conservare i supporti di back-up relativi alle banche dati delle applicazioni sw gestite.
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria				X		Il Comune ha installato e mantiene un impianto antincendio; ha provveduto a sollevare i PC da terra contro il rischio di allagamento. Occorre fronteggiare ulteriormente il rischio attuando il Piano di Disaster & Recovery e Continuità Operativa.
	Valore Medio			**X**			

Legenda:

IMPATTO: 0= impatto basso; 1= impatto medio; 2=impatto alto, aspetto importante; 3= impatto molto alto; aspetto fondamentale

CRITICITA': 0= criticità basso; 1= criticità medio; 2= criticità alto, aspetto importante; 3= criticità molto alto; aspetto fondamentale

5.4 Sintesi dei rischi

Il grafico seguente sintetizza il livello di rischio rispetto agli aspetti analizzati in precedenza.

Nella tabella seguente si riporta l'acronimo del relativo aspetto analizzato nelle tabelle impatto precedenti (es. Unah: Uso non autorizzato dell'hardware) nella posizione intercettata dal valore dell'impatto identificato, con il valore medio dei relativi fattori di rischio analizzati nella tabella analisi del rischio.

Legenda:

Unah: Uso non autorizzato hw
Riin: Rivelazione illegittima di Informazioni , anche per negligenza
Anai: Alterazione non autorizzata di Informazioni
Prin: Perdita di informazioni
Unai:Uso non autorizzato di informazioni
Unaa: Uso non autorizzato di applicativi
Psup: Perdita o riutilizzo di supporti cartacei o magnetici o documentazioni accessorie

Area Critica

Impatto					
	3		Riin	**Prin**	
	2		Unai Unaa Unah Psup	**Anai**	
	1				
	0				
		0	1	2	3

Criticità

6 Piano di adeguamento

In questo capitolo viene presentato il piano di adeguamento adottato dalla AOO a seguito dell'analisi dei rischi effettuata, in termini di:

- misure di sicurezza adottate
- misure di sicurezza da adottare

Nella tabella seguente si riporta una sintesi degli aspetti critici per la sicurezza dell'Ente e vengono, inoltre, indicati i trattamenti, o contromisure da adottare, per fronteggiare e mantenere sotto controllo ciascuna di tali criticità.

La tabella che segue costituisce la sintesi dell' analisi dei rischi effettuata ed è molto importante perché riassume tutte le principali azioni da intraprendere per raggiungere il traguardo della protezione dei documenti trattati dall'Ente e dei dati personali in essi contenuti.

Misure di sicurezza adottate e da adottare

Macro categoria di rischio	Fattore di rischio	Misure in essere	Misure da adottare	Priorità	Tipo di adeguamento
ANAI	•Furto di credenziali di autenticazione	Il comune ha realizzato un progetto per la configurazione completa della rete e, quindi, gli incaricati sono dotati di credenziali di autenticazione per l'accesso alla rete.	Occorre incaricare un custode delle password e predisporre istruzioni operative sull'uso corretto delle credenziali. L'Amministrazione comunale ha programmato un corso di	Massima	Logico Organizzativo

		Le credenziali di autenticazione rispondono ai requisiti richiesti dal D.Lgs. 196/03 – Allegato B.	formazione agli incaricati che sarà erogato nell'anno in corso.		
PRIN ANAI	•Carenza di consapevolezza, disattenzione o incuria •Errori umani		Programmare interventi di formazione e/o informazione agli incaricati sulla sicurezza dei dati, estesi anche alle tecnologie ed applicazioni in uso presso l'Ente. Predisporre, adottare e distribuire linee guida, procedure organizzative, mansionari ed informativa ai dipendenti.	Alta	Organizzativo
PRIN	•Malfunzionamento, indisponibilità o degrado degli strumenti	Esiste contratto di manutenzione attivo con le Ditte fornitrici delle applicazioni sw. E' stato attivato un supporto di assistenza e manutenzione dell'infrastruttura di comunicazione e degli strumenti. E' stato affidato l'incarico di amministratore informatico ad un tecnico esterno che garantisce la disponibilità dei dati tramite un adeguato programma di back up e recovery.	Occorre che il responsabile informatico continui nelle azioni di organizzazione, controllo e garanzia sulla piena disponibilità dei dati, sul buon funzionamento degli strumenti di sicurezza installati, della rete e di tutta la strumentazione hw e sw configurata in rete. Il responsabile informatico deve garantire il tracciamento degli accessi dell'amministratore di sistema e controllarne l'operato periodicamente. Occorre attuare il piano di disaster & recovery e continuità operativa.	Alta	Logico, fisico ed organizzativo
ANAI	•Comportamenti sleali o fraudolenti	E' stato installato un firewall che permette il tracciamento di qualsiasi tentativo di intrusione sulla rete LAN del Comune. Sono state attivate firma digitale e posta elettronica certificata sui documenti elettronici con validità probatoria.	Proteggere documenti con dati sensibili e giudiziari salvandoli in modo criptato.	Alta	Organizzativo e logico
PRIN	•Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	I computer sono protetti da allagamenti, perché installati su un carrellino e quindi sollevati da terra. E' stato installato e viene verificato periodicamente l'impianto antincendio ai sensi della L. 626/94. Viene effettuato il back up giornaliero delle banche dati. E' stato predisposto un piano di disaster & recovery e continuità operativa su cui la ex DigitPA ha espresso parere favorevole.	Occorre destinare un luogo sicuro (ad es. cassaforte ignifuga posta in un luogo sicuro lontano dalla sede del server) per la conservazione dei supporti su cui vengono salvati i dati. Occorre passare all'attuazione del piano di disaster & recovery e continuità operativa.	Alta	Logico Organizzativo
PRIN	•Guasto tecnologico ai sistemi complementari	Sono stati installati i gruppi di continuità su tutti i server e le postazioni di lavoro.	Rafforzare le misure di protezione ai sistemi informativi, adeguando tali sistemi con dispositivi di allarme che possano prevenire gravi conseguenze agli strumenti elettronici ospitati. Attuare il Piano di Disaster & Recovery e Continuità Operativa	Alta	Fisico
PRIN ANAI	•Azioni di virus informatici o codici malefici su strumenti connessi e non alla rete	Il Comune ha realizzato un progetto per il collegamento in rete di tutti i PC e l'installazione di un antivirus centralizzato sul server che aggiorna quotidianamente tutte le postazioni di lavoro del Comune. E' stato incaricato un amministratore informatico che ha la responsabilità di garantire	Stabilire idonee politiche di sicurezza per ciò che riguarda l'aggiornamento delle patch di Microsoft che non risultano sempre aggiornate sulle postazioni di lavoro.	Media	Logico

		il buon funzionamento dei servizi in oggetto.			
ANAI PRIN	•Accessi esterni non autorizzati •Asportazione e furto di strumenti contenenti dati	La sede principale è dotata di guardiania e l'ingresso agli uffici da parte di persone estranee è controllato strettamente. Le finestre e i balconi situati a piano terra sono protetti da inferriate. Le porte degli uffici sono state dotate di serrature idonee e funzionanti.	Attuare il Piano di Disaster & Recovery e Continuità Operativa	Bassa	Fisico

Nella tabella seguente si effettua, per ogni macro-categoria di rischio, una valutazione dell'impatto che hanno le relative contromisure da adottare sui tre tipi di adeguamento:

- logico
- organizzativo
- fisico

La valutazione deriva anche dalle motivazioni espresse nell'analisi dei rischi.

Macro categoria di rischio	Impatto		
	Adeguamento Logico	Adeguamento Organizzativo	Adeguamento Fisico
PRIN: Perdita di Informazioni	**3**	2	0
ANAI: Alterazione non autorizzata di informazioni	**1**	**2**	0