

**COMUNE DI
AZZATE**

**MANUALE DEL PROTOCOLLO
INFORMATICO E GESTIONE
DOCUMENTALE A NORMA**

ADOTTATO DALL'ENTE

All13ManProtDoc

Rev. 03

del 20.05.2025



COMUNE DI AZZATE
Provincia di Varese
Ufficio Affari Generali

ALLEGATO13

AL MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

PIANO PER LA SICUREZZA INFORMATICA

Piano di sicurezza dei documenti informatici

Fatto salvo che la gestione dei flussi documentali dell'ente a far data dal 24.10.2024 è stata trasferita nella versione cloud presso la società fornitrice del sistema gestionale in uso all'ente, denominata SISCOP-Nuvola, alla quale è demandata la gestione della sicurezza informatica e contestuale salvataggio e conservazione dei dati, mediante stipula di specifico contratto di trattamento dati, a seguito appalto del servizio medesimo, si descrivono le azioni intraprese da questo Comune per assicurare la sicurezza.

1 Accesso da parte degli uffici utente

La riservatezza della registrazione del protocollo è garantita dal sistema attraverso l'uso di profili utente e password, e dalla profilazione di ciascun operatore all'interno del sistema che delinea in base ai ruoli rivestiti permessi puntuali e specifici per le competenze attribuite, gestiti dall'Amministratore del servizio messo in rete sul cloud.

2 Piano di sicurezza dei documenti informatici

Il Comune di Azzate ha adottato le seguenti misure di sicurezza, raggruppandole in 3 aree:

- Sicurezza fisica
- Sicurezza logica
- Sicurezza delle apparecchiature hardware
- Sicurezza organizzativa
- **Sicurezza fisica:**
 1. Il sistema informatico del computer è completamente contenuto in un unico luogo, a cui fanno capo le reti di telecomunicazioni sia pubbliche che private,
 2. Le chiavi d'accesso ai locali sono distribuite ai dipendenti/responsabili del servizio, agli Amministratori dell'Ente (Giunta) e al Segretario comunale,
 3. Presenza di estintori adeguati.
- **Sicurezza delle apparecchiature hardware**
 1. L'isolamento della sala server garantisce la protezione dell'apparecchiatura da danneggiamenti. Il suo impianto di alimentazione è protetto da un gruppo di continuità.
 2. L'impianto di alimentazione è sezionato a seconda del tipo di strumentazione che deve essere gestita. Il server mantiene un controllo logico sullo stato di alimentazione ed è in grado di segnalare agli utenti collegati la mancanza di corrente, dopo un ragionevole lasso di tempo in stato di blackout, il sistema procede allo spegnimento automatico per evitare danni alle apparecchiature.
 3. Tutti i dispositivi classificati "di sistema" (server, apparati attivi di rete, firewall...) sono coperti da un servizio di manutenzione che garantisce tempi di intervento adeguati per il ripristino degli apparati.
 4. Deposito in altro luogo sicuro delle copie di sicurezza dei dati.
- **Sicurezza logica**
 1. Per sistema di sicurezza logica si intende il sistema di sicurezza dell'architettura informatica, dotato quindi di meccanismi opportuni e di specifiche funzioni di gestione e controllo.

2. Il sistema informatico comunale è basato su un meccanismo che costringe ogni utente ad autenticarsi (dimostrare la propria identità) prima di poter accedere a un calcolatore.
3. Ogni utente è associato ad una password univoca disabilitata dagli amministratori qualora non più autorizzata.
4. Ogni utente/dipendente può accedere ad un'area di lavoro riservata per il/i settore/settori di appartenenza.
5. Disattivazione della password in caso di perdita di qualità legittimante l'accesso o per mancato utilizzo per oltre un anno.
6. Il sistema antivirus è attivo sul server, sulle stazioni utenti e sul servizio di posta elettronica. Controlla ogni flusso di informazioni tra le parti, in particolare l'antivirus per la posta elettronica esegue il controllo degli allegati e inibisce anche l'accesso alla rete del comune ad allegati di tipo pericoloso indipendentemente che contengano virus conosciuti; aumentando quindi il livello di sicurezza. Lo scarico di aggiornanti dal sito del produttore sono schedulati ogni notte e non richiedono attività da parte dell'utente.
7. Backup giornaliero e controllo dell'avvenuto salvataggio.
8. I supporti di memorizzazione costantemente controllati per la loro funzionalità, sono conservati in un luogo separato.

• **Sicurezza organizzativa**

Gli aspetti organizzativi riguardano principalmente la definizione di ruoli, compiti e responsabilità per la gestione di tutte le fasi del processo Sicurezza e l'adozione di specifiche procedure che vadano a completare e rafforzare le contromisure tecnologiche adottate.

Il Responsabile dell'Ente preposto (a cui sono assegnate le risorse finanziarie specifiche) propone hardware di implementazione del Sistema informatico.

Gli interventi sui software di tipo gestionale installati da diversi fornitori sono gestiti con incarico di assistenza e aggiornamento da fornitori/concessionari.

• **Produzione e conservazione delle registrazioni di protocollo informatico**

Ogni registrazione di protocollo è generata nel momento in cui l'operatore, avendo inserito i dati relativi al documento che sta protocollando, conferma l'inserimento: il sistema genera un nuovo numero di protocollo e attribuisce automaticamente la data e l'ora di protocollazione. Ciascuna registrazione produce un apposito record sul sistema centrale che viene accordato in una base dati.

La procedura del protocollo informatico è collegata automaticamente ad un sistema di segnatura da apporre sui documenti (e relativi allegati) contenente tutti i dati del relativo numero di protocollo.

Le registrazioni possono essere modificate nei dati relativi, ad esempio, al codice di classificazione, al tipo di spedizione, alle annotazioni, all'ufficio di carico e al responsabile del documento.

A norma dell'articolo 53 del DPR 455/2000, la procedura del protocollo è impostata in modo che il numero di protocollo, la data e l'ora di protocollazione vengano assegnate automaticamente dal sistema e non siano modificabili in sede di variazione delle registrazioni, così come il mittente o il destinatario e l'oggetto del documento.

L'annullamento di una registrazione errata, viene effettuato tramite una procedura che richiede l'indicazione del numero e della data del provvedimento di autorizzazione all'annullamento (registrato in apposito registro nel sistema gestionale).