



# Comune di Redavalle (PV)

## MANUALE DI GESTIONE DOCUMENTALE E DELLA CONSERVAZIONE

### *Allegato 08 – Piano per la Sicurezza Informatica*

## PIANO PER LA SICUREZZA INFORMATICA

### 1. Premessa e ambito di applicazione

Il presente piano di sicurezza è adottato ai sensi delle Linee Guida AgID sulla formazione, gestione e conservazione del documento informatico, nonché del Regolamento UE 2016/679 (GDPR). Esso descrive le politiche adottate dall'Ente affinché:

- I documenti e le informazioni trattati siano resi disponibili, integri e riservati.
- I dati personali comuni, sensibili e giudiziari vengano custoditi in modo da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito.

Il piano definisce le misure tecniche, organizzative e procedurali per la tutela del patrimonio documentale gestito attraverso il sistema SISCOM NuvolaComuni.

### 2. Analisi dei rischi

I documenti informatici e i dati gestiti dal Sistema di Gestione Informatica dei Documenti (SGID) sono esposti a rischi che possono comprometterne la validità giuridica o la riservatezza. Le principali minacce identificate includono:

- **Accesso non autorizzato:** Intrusione nel sistema o visualizzazione indebita di fascicoli riservati.
- **Manomissione o Cancellazione:** Modifica non tracciata dei dati di protocollo o eliminazione accidentale di documenti.
- **Perdita dei dati:** Indisponibilità dovuta a guasti tecnici o eventi calamitosi.
- **Trattamento illecito:** Utilizzo dei dati per finalità non conformi ai compiti istituzionali.

### 3. Infrastruttura tecnologica e sicurezza della rete

Il Sistema di Gestione Informatica dei Documenti in uso è SISCOM NuvolaComuni. L'architettura non risiede su server fisici esposti vulnerabilmente, ma è basata su un modello SaaS (Software as a Service) erogato in modalità Cloud.

#### 3.1 Qualificazione e sicurezza Cloud

L'infrastruttura tecnologica risponde ai requisiti del "Cloud della PA":



# Comune di Redavalle (PV)

## MANUALE DI GESTIONE DOCUMENTALE E DELLA CONSERVAZIONE

### **Allegato 08 – Piano per la Sicurezza Informatica**

- È qualificata nel Marketplace dei servizi Cloud per la PA dell'Agenzia per la Cybersicurezza Nazionale (ACN).
- È certificata secondo gli standard internazionali di sicurezza ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018.
- Garantisce l'applicazione delle misure minime di sicurezza ICT per le Pubbliche Amministrazioni (Circolare AgID n. 2/2017 e ss.mm.ii.).

L'accesso al sistema avviene tramite protocollo sicuro (HTTPS) ed è riservato alle postazioni o agli utenti autenticati, ereditando i meccanismi di protezione perimetrale dell'infrastruttura Cloud certificata.

#### **4. Politiche di gestione degli accessi e delle credenziali**

##### **4.1 Identificazione e autenticazione**

L'accesso al sistema SISCOM è consentito esclusivamente previa procedura di identificazione informatica. A ogni incaricato sono assegnate credenziali personali costituite da:

- User-ID: Codice identificativo univoco.
- Password: Parola chiave riservata, nota solo all'utente.

Per l'utente in possesso di sistemi di identificazione digitale, è possibile accedere allo SGID NuvolaComuni anche tramite CIE e SPID.

##### **4.2 Profilazione degli utenti Interni**

L'accesso ai documenti non è indiscriminato ma regolato dal principio di necessità (*need to know*). Il sistema gestisce l'assegnazione dei diritti tramite profili di autorizzazione predefiniti.

- Ogni utente visualizza e gestisce di norma solo i documenti assegnati alla propria UOR o ai propri procedimenti di competenza.
- La visibilità su fascicoli di altri uffici è inibita di default e può essere concessa solo esplicitamente dal Responsabile del procedimento o dell'UOR competente.
- Le funzioni di amministrazione del sistema (creazione utenti, modifica log, configurazione) sono riservate esclusivamente agli Amministratori di Sistema e al Responsabile della Gestione Documentale.



# Comune di Redavalle (PV)

## MANUALE DI GESTIONE DOCUMENTALE E DELLA CONSERVAZIONE

### *Allegato 08 – Piano per la Sicurezza Informatica*

#### 4.3 Password policy

In conformità alle best practice di sicurezza, la password deve rispettare i seguenti requisiti di complessità:

- Lunghezza minima di 8 caratteri.
- Composizione mista contenente almeno una lettera maiuscola, una minuscola, un numero e un carattere speciale (simbolo non alfanumerico).
- Assenza di riferimenti agevolmente riconducibili all'utente (es. nome, data di nascita).

#### 4.4 Ciclo di vita delle credenziali

- **Modifica periodica:** La password deve essere modificata al primo utilizzo e successivamente con cadenza obbligatoria trimestrale.
- **Disattivazione:** Le credenziali non utilizzate per un periodo superiore a sei mesi vengono disattivate automaticamente dal sistema. I profili disattivati non possono essere riattivati; in caso di rientro in servizio, sarà necessaria una nuova assegnazione.
- **Smarrimento:** In caso di dimenticanza, si procede al reset e all'assegnazione di una nuova chiave di accesso; la vecchia password non è recuperabile.

#### 4.5 Procedura di emergenza

Per garantire la continuità amministrativa nel trattamento di dati sensibili o giudiziari, le credenziali degli operatori abilitati a tali trattamenti devono essere consegnate in busta chiusa e sigillata al Responsabile della UOR. L'apertura della busta è consentita al Responsabile solo in casi di necessità indifferibile (es. assenza prolungata e imprevista dell'operatore) per garantire l'operatività dell'ufficio. Al rientro, l'operatore dovrà generare una nuova password e consegnare una nuova busta sigillata.

#### 4.6 Accesso di utenti esterni

L'accesso da parte di soggetti esterni all'Amministrazione (cittadini, imprese, altre PA) è consentito secondo modalità differenziate:

- **Accesso autenticato:** Richiesto per la consultazione di pratiche specifiche o dati non divulgabili. L'utente esterno deve essere preventivamente censito e dotato di credenziali, oppure autenticarsi tramite sistemi di identità digitale (SPID/CIE).



# Comune di Redavalle (PV)

## MANUALE DI GESTIONE DOCUMENTALE E DELLA CONSERVAZIONE

### *Allegato 08 – Piano per la Sicurezza Informatica*

- **Consultazione pubblica:** Per i dati soggetti a pubblicità legale (Albo Pretorio) o trasparenza, l'accesso avviene tramite il sito web istituzionale in formato aperto, garantendo comunque il rispetto della normativa sulla protezione dei dati personali (oscuramento dati sensibili ove previsto).

#### **5. Sicurezza delle postazioni di lavoro e comportamento degli operatori**

Le postazioni di lavoro sono strumenti istituzionali. Agli operatori è fatto obbligo di:

1. **Custodia:** Non lasciare mai la postazione incustodita con la sessione aperta. È obbligatorio bloccare o spegnere il PC in caso di allontanamento temporaneo o al termine del servizio.
2. **Protezione Visiva:** Adottare accorgimenti (es. posizionamento monitor) per evitare che dati personali siano visibili a terzi non autorizzati, specialmente in uffici aperti al pubblico.
3. **Divieti:** Non installare software non autorizzato e non copiare dati di titolarità dell'Ente su dispositivi personali esterni (chiavette USB, hard disk personali).
4. **Segnalazione:** Comunicare immediatamente ai referenti tecnici qualsiasi anomalia o sospetta violazione della sicurezza.

#### **6. Sicurezza nella formazione e gestione del documento**

##### **6.1 Formati e firma digitale**

I documenti informatici sono prodotti nei formati standard previsti dalle Linee Guida AgID (es. PDF/A) atti a garantire l'immutabilità e la leggibilità nel tempo. La sottoscrizione con firma digitale avviene prima della registrazione di protocollo per garantire paternità e integrità del documento.

##### **6.2 Integrità del Protocollo**

Il sistema SISCOM NuvolaComuni garantisce l'immodificabilità delle registrazioni chiave (numero, data, oggetto, mittente/destinatario).

- **Logging:** Ogni operazione, inclusa l'eventuale modifica autorizzata di campi secondari, è tracciata in file di log che registrano autore, data, ora e tipo di operazione, mantenendo recuperabile la versione precedente.



# Comune di Redavalle (PV)

## MANUALE DI GESTIONE DOCUMENTALE E DELLA CONSERVAZIONE

### ***Allegato 08 – Piano per la Sicurezza Informatica***

- **Annullamento:** L'annullamento di una registrazione è consentito solo previa autorizzazione formale e il sistema ne conserva traccia indelebile.
- **Registro Giornaliero:** Al termine di ogni giornata, il sistema genera automaticamente il Registro Giornaliero di Protocollo in formato statico, che viene inviato in conservazione entro il giorno successivo.

#### **7. Backup e continuità operativa (Disaster Recovery)**

Al fine di prevenire la perdita dei dati, l'Ente adotta una strategia di backup e ripristino basata sulla ridondanza e sulla sicurezza del Cloud, integrando le procedure del fornitore SISCOM.

##### **7.1 Gestione dei Backup**

- **Dati in Cloud:** Il backup dei dati contenuti nel Sistema SISCOM Nuvola avviene in modalità automatica direttamente sull'infrastruttura Cloud certificata, garantendo la replicazione geografica e la sicurezza fisica dei data center.
- **Disaster Recovery:** L'Ente, tramite il fornitore, dispone di un sistema di *Disaster Recovery* in grado di garantire il ritorno alla normale operatività anche in caso di eventi critici, prevedendo il ripristino dei dati dalle copie in cloud nell'arco temporale stabilito dalla convenzione di servizio (SLA) e nel rispetto della normativa vigente.

##### **7.2 Conservazione a lungo termine**

I documenti informatici definitivi sono versati nel sistema di conservazione digitale a norma, gestito da un Conservatore Accreditato AgID esterno (ARUBA Spa). Il versamento avviene tramite pacchetti di versamento (SIP) standardizzati, garantendo la preservazione del valore legale dei documenti per il tempo previsto dal massimario di scarto.

#### **8. Tutela dei dati e gestione delle violazioni (Data Breach)**

##### **8.1 Misure per dati sensibili e giudiziari**

Il trattamento di categorie particolari di dati (art. 9 e 10 GDPR) richiede misure rafforzate. Ove tecnicamente possibile, il sistema applica tecniche di cifratura o pseudonimizzazione (uso di codici identificativi) per separare i dati identificativi dalle informazioni sensibili. Anche



# Comune di Redavalle (PV)

## MANUALE DI GESTIONE DOCUMENTALE E DELLA CONSERVAZIONE

### **Allegato 08 – Piano per la Sicurezza Informatica**

per gli archivi cartacei e ibridi, l'accesso ai fascicoli riservati è consentito solo previa autorizzazione e registrazione dell'accesso.

#### **8.2 Trasmissione sicura dei documenti**

La trasmissione interna di documenti avviene esclusivamente tramite il flusso di lavoro (*workflow*) del SGID per evitare duplicazioni e dispersioni via e-mail. La trasmissione esterna verso altre PA o privati avviene tramite canali sicuri e certificati (PEC, interoperabilità SPC) utilizzando le signature XML conformi agli standard nazionali. È vietato utilizzare canali non istituzionali (es. e-mail personali, servizi di file transfer non approvati) per la trasmissione di documenti dell'Ente.

#### **8.3 Notifica delle violazioni**

In caso di violazione di sicurezza che comporti la perdita, la distruzione o la divulgazione non autorizzata di dati personali (*Data Breach*), il Responsabile del Trattamento notifica l'accaduto al Garante per la Protezione dei Dati Personali entro 72 ore dalla scoperta, ai sensi dell'art. 33 del GDPR. Se la violazione comporta rischi elevati per i diritti degli interessati, l'Ente provvederà a comunicare l'accaduto anche a questi ultimi (art. 34 GDPR).

### **9. Formazione, monitoraggio e revisione**

#### **9.1 Formazione del personale**

L'Ente predispone piani di formazione periodici per tutto il personale autorizzato. La formazione copre l'utilizzo tecnico del SGID, le procedure di sicurezza, la normativa sulla privacy e la gestione documentale.

#### **9.2 Monitoraggio e Audit**

Il Responsabile della Gestione Documentale effettua controlli periodici, anche a campione, per verificare:

- La corretta tenuta dei registri e dei log di sistema;
- La coerenza dei profili di autorizzazione assegnati;



# Comune di Redavalle (PV)

## MANUALE DI GESTIONE DOCUMENTALE E DELLA CONSERVAZIONE

### *Allegato 08 – Piano per la Sicurezza Informatica*

- Il rispetto delle procedure di sicurezza da parte degli utenti. I file di log del sistema sono conservati in modalità sicura e possono essere messi a disposizione dell'Autorità Giudiziaria in caso di indagini.

#### **9.3 Revisione del piano**

Il presente Piano di Sicurezza è soggetto a revisione con cadenza almeno biennale, o anticipata in caso di significative modifiche normative, organizzative o tecnologiche.