

Sistema di Protocollazione Suite NettunoPA: Specifiche Tecnico-Operative e Standard di Sicurezza delle Informazioni

Il presente documento definisce le specifiche funzionali, architetturali e i requisiti di sicurezza relativi al sistema di protocollazione digitale della suite **NettunoPA** (indicata anche come Nettuno PA), configurato in conformità agli standard richiesti per le Pubbliche Amministrazioni e per organismi di rilievo istituzionale come Unioncamere.

1. Descrizione Generale del Protocollo Digitale Web

Il modulo **Protocollo Digitale Web**, parte integrante della Suite Segreteria Digitale di NettunoPA, è un software nativamente Cloud progettato per consentire la completa digitalizzazione di tutti i flussi documentali che transitano dagli uffici di protocollo della Pubblica Amministrazione. Il sistema è orientato a semplificare il lavoro quotidiano, ottimizzare la condivisione tra più utenti in rete e garantire un'archiviazione automatica e sicura.

Funzionalità Chiave

- **Integrazione nativa con la PEC (Posta Elettronica Certificata):** Consente il caricamento e la protocollazione automatica non solo del messaggio principale, ma anche di tutti i file allegati.
- **Gestione del cartaceo:** Fornisce moduli dedicati all'acquisizione digitale tramite scanner e all'importazione di file da percorsi locali per i documenti sprovvisti di canali telematici automatici.
- **Profili utente e protocolli riservati:** Abilita una gestione granulare dei permessi, consentendo di limitare l'operatività del personale (es. solo protocolli in entrata o in uscita) e garantendo che i protocolli riservati siano gestiti in totale riservatezza, pur mantenendo una numerazione unica e sequenziale.
- **Tracciabilità totale:** Registra in maniera persistente e imm modificabile l'autore di ogni inserimento o modifica sul sistema.

2. Architettura e Conservazione Sostitutiva

Per soddisfare i requisiti normativi dettati dall'AgID (Agenzia per l'Italia Digitale) in materia di protocollo informatico (DPCM 3 Dicembre 2013), il sistema adotta un'infrastruttura robusta focalizzata sulla conservazione a norma del registro giornaliero di protocollo.

Componente Architetturale	Caratteristiche e Funzioni
Infrastruttura Cloud	Erogazione in modalità Software-as-a-Service (SaaS), accessibile anche tramite identità

Componente Architettuale	Caratteristiche e Funzioni
	digitale (SPID/CIE).
Backup e Ridondanza	Auto-salvataggi configurati in tempo reale su personal computer, server di rete locali e archivi Cloud distribuiti.
Conservazione Certificata AgID	Integrazione nativa con conservatori accreditati AgID per l'invio e l'archiviazione sostitutiva a norma di legge dei registri e dei file in formato idoneo (es. PDF firmati digitalmente).

3. Framework di Sicurezza delle Informazioni (SGSI)

La suite opera sotto un rigoroso Sistema di Gestione della Sicurezza delle Informazioni (SGSI) strutturato in conformità alle norme internazionali **ISO/IEC 27001:2022**, **ISO/IEC 27017:2015** (controlli cloud), **ISO/IEC 27018:2019** (protezione PII nel cloud pubblici) e alla **Direttiva NIS2**. Questo quadro garantisce i tre pilastri fondamentali della sicurezza informatica:

- **Riservatezza:** Accessibilità dei dati limitata esclusivamente al personale autorizzato e prevenzione di accessi o divulgazioni non regolamentate.
- **Integrità:** accuratezza e completezza delle informazioni e delle modalità di elaborazione, con modifiche tracciate e autorizzate secondo procedure controllate.
- **Disponibilità:** Accesso tempestivo e garantito agli asset informativi da parte degli utenti autorizzati, supportato da procedure di continuità operativa.

Ruoli e Responsabilità di Sicurezza

L'organizzazione della sicurezza per i servizi della suite prevede compiti ben definiti a livello di governance:

- **Top Management & Presidente C.d.A.:** Guidano l'impegno istituzionale, approvano i piani di trattamento dei rischi e forniscono le risorse necessarie al mantenimento del sistema.
- **Responsabile del Sistema di Gestione:** Sovrintende all'attuazione, al monitoraggio e alla valutazione dei rischi informatici, riferendo direttamente alla direzione.
- **Chief Financial Officer (C.F.O.):** Designato formalmente come punto di contatto ufficiale per le questioni inerenti alla cybersecurity.
- **Responsabile Risorse Umane:** Verifica l'esperienza e l'affidabilità del personale prima di concedere l'accesso ai sistemi sensibili, assicurando la firma di Accordi di Non Divulgazione (NDA).

Principi Operativi di Sicurezza per il Personale

Gli utenti della PA che operano sul registro di protocollo sono tenuti all'osservanza di rigide regole operative:

1. **Politica della Scrivania e dello Schermo Puliti:** Protezione fisica di informazioni sensibili o supporti rimovibili quando inutilizzati. Blocco automatico della postazione di lavoro con autenticazione obbligatoria dopo brevi periodi di inattività.
2. **Lavoro da remoto sicuro:** Utilizzo dei dispositivi mobili e del telelavoro subordinato alle misure di sicurezza prescritte per mitigare il rischio di furto, smarrimento o intercettazione

dei dati fuori sede.

3. **Segnalazione Tempestiva:** Obbligo per tutto il personale di segnalare immediatamente qualsiasi evento, anomalia o vulnerabilità riscontrata sui canali ufficiali della piattaforma.

4. Interconnessione e Flussi Ecosistemici della PA

Il sistema di protocollazione funge da nucleo centrale per altri applicativi verticali della PA. È nativamente integrato con i moduli di *Amministrazione Trasparente* e *Albo Pretorio* per consentire la pubblicazione immediata degli atti amministrativi richiesti dalle normative vigenti (es. Dlgs 33/2013 e Legge 69/2009), riducendo drasticamente i tempi di caricamento manuale e massimizzando l'efficienza dei flussi di lavoro negli enti complessi come Unioncamere.