ALLEGATO D: Gestione documentale informatica

Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso, pubblica *(UserID)* e privata *(Password)* 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. Queste, in sintesi, sono:

- *consultazione,* per visualizzare in modo selettivo, le registrazioni di protocollo eseguite da altri;
- *inserimento,* per inserire gli estremi di protocollo e effettuare una registrazione di protocollo ed associare i documenti;
- *modifica,* per modificare i dati opzionali di una registrazione di protocollo;
- *annullamento,* per annullare una registrazione di protocollo autorizzata dal RSP.

Le regole per la composizione delle *password* e il blocco delle utenze valgono sia per gli amministratori delle AOO che per gli utenti delle AOO.

Le relative politiche di composizione, aggiornamento e, in generale di sicurezza, sono configurate sui sistemi di accesso come obbligatorie e gestite come previsto nelle MMS.

Il Sistema di Protocollo (SdP) fruito dall'AOO:

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

Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, viene associata una *Access Control List* (ACL) che consente di stabilire quali utenti, o gruppi di utenti, hanno accesso ad esso (sistema di autorizzazione o profilazione utenza).

Considerato che il SdP segue la logica dell'organizzazione, ciascun utente può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli Uffici Utente (UU) ad esso subordinati.

Il sistema consente, altresì, di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'AOO.

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio o di una ricerca *full text.*

Utenti interni alla AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal RSP dell'AOO.

Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla cancellazione e alla modifica delle informazioni.

La gestione delle utenze rispetta i seguenti principi operativi:

- gli utenti creati non sono mai cancellati ma, eventualmente, disabilitati (su richiesta esplicita dell'amministratore dell'AOO o per errori di inserimento)
- la credenziale privata degli utenti e dell'amministratore AOO non transita in chiaro sulla rete, né al momento della prima generazione, né successivamente al momento del login.

Accesso al registro di protocollo per utenti interni alla AOO

L'autorizzazione all'accesso ai registri di protocollo è regolata tramite i seguenti strumenti:

- liste di competenza, gestite dall'amministratore di AOO, per la definizione degli utenti abilitati ad accedere a determinate voci del titolario;
- ruoli degli utenti, gestiti dall'amministratore di ente (amministrazione), per la specificazione delle macro-funzioni alle quali vengono abilitati;
- protocollazione "particolare o riservata", gestita dall' amministratore di ente, relativa a documenti sottratti alla consultazione da parte di chi non sia espressamente abilitato.

La visibilità completa sul registro di protocollo è consentita soltanto all'utente con il profilo di utenza di “Operatore di protocollo” o "Responsabile del registro" e limitatamente al registro dell'AOO sul quale è stato abilitato ad operare.

L'utente assegnatario dei documenti protocollati è invece abilitato ad una vista parziale sul registro di protocollo. Tale vista è definita dalle voci di titolario associate alla lista di competenza in cui l'utente è presente (sia come singolo, sia come ufficio).

Conservazione dei documenti informatici

La conservazione dei documenti informatici avviene sulla base delle disposizioni riportate nel:

- DPCM 13 novembre 2014, per quanto attiene ai documenti informatici presenti nell’archivio corrente dell’Agenzia
- DPCM 3 dicembre 2013 per i documenti inviati in conservazione.

Servizio archivistico

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l’immodificabilità del contenuto. Al riguardo di seguito si descrivono le modalità di produzione di invio in conservazione delle registrazioni di protocollo informatico con l’indicazione delle soluzioni tecnologiche ed organizzative adottate per garantire l’immodificabilità della registrazione medesime. Tali modalità sono riportate nel manuale di conservazione dell’AgID

Il SdP provvede all’esecuzione automatica della stampa su file in formato PDF del Registro giornaliero di protocollo. Il documento così creato riporta su un unico file con estensione .PDF il riepilogo di tutte le registrazioni di protocollo eseguite nell’ambito della medesima giornata e, a seguire, gli eventuali annullamenti (parziali o totali) occorsi ai protocolli acquisiti nel corso dei giorni precedenti.

Per quanto attiene ai metadati da inviare in conservazione unitamente alla copia del registro di cui sopra, sono stati suddivisi in tre sottogruppi:

● Metadati di identificazione. Contengono le informazioni relative all'ente che sta inviando il documento (File.PDF) al conservatore e quelle del protocollo che identificano univocamente il documento. Sono memorizzati tra le proprietà del sistema (Ente, struttura, ecc.) e sulla registrazione del documento.

● Metadati di profilo generali. Contengono le informazioni generali sul documento, come oggetto e data. Sono memorizzati sulla registrazione di protocollo.

● Metadati di profilo specifici. Contengono le informazioni specifiche del tipo di documento, come numero di protocolli effettuati nella giornata, numero iniziale e numero finale. Sono memorizzati sulla registrazione di protocollo e tra le proprietà dell'Area Organizzativa Omogenea. La produzione del documento avviene dopo la chiusura del Registro di protocollo e prima della riapertura al giorno successivo in modo che nessun altro documento possa essere protocollato nel registro della giornata precedente né in modalità manuale né in modalità automatica.

All'avvio del processo di creazione del pacchetto di versamento vengono elaborati i dati presenti nel registro di protocollo al fine di:

1. Ottenere i metadati di profilo specifici da inviare al sistema di conservazione (Numero iniziale, Numero Finale, Data inizio registrazione, Numero di documenti registrati, Numero di documenti annullati).
2. Effettuare la registrazione del file PDF nel registro/repertorio stabilito e memorizzare tra gli attributi estesi del documento quelli calcolati precedentemente.
3. Predisporre il documento all'invio in conservazione indicando lo stato "da conservare".
4. In caso di anomalia durante il flusso inviare una notifica al responsabile della conservazione.

Il trasferimento del Pacchetto di versamento al sistema di conservazione avviene tramite canale WebServices.

Al riguardo è previsto un processo automatico che si occupi di creare il pacchetto di versamento, inviarlo al sistema di conservazione e registrare lo stato del versamento stesso. Il processo provvede a:

1. Estrarre dal registro giornaliero il documento da inviare in conservazione. In generale è presente un solo documento da inviare ma nel caso sia avvenuto un problema nei giorni precedenti la procedura effettua l'invio di tutti i documenti in attesa.
2. Predisporre il pacchetto di versamento estraendo le informazioni necessarie dal documento e dal sistema.
3. Inviare il pacchetto in modalità sincrona.
4. In caso di esito positivo indicare nel documento lo stato "conservato".
5. In caso di esito negativo indicare nel documento lo stato "errore" ed inviare una notifica al responsabile della conservazione

Nelle more di avvio del servizio di invio in conservazione sopra descritto il file PDF del registro giornaliero è registrato nel registro di protocollo interno dell'Agenzia a tutela della immodificabilità del medesimo ai sensi dell'art.3, comma 4, lettera d), del DPCM 13 novembre 2014.

Formazione dei documenti - Aspetti attinenti alla sicurezza

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'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 con AOO diverse.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o text editor che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano preferibilmente i formati PDF/A, XML e TIFF.
I documenti informatici redatti dall'AOO con altri prodotti di text editor sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF/A, 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 della 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 13 novembre 2014 ("Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici").

Gestione dei documenti informatici

Il sistema operativo delle risorse elaborative destinate ad erogare il servizio di protocollo informatico è conforme alle specifiche previste dalla normativa vigente. Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in maniera da consentire:

- l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso.
- Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate. Il sistema di gestione informatica dei documenti:
- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy", con particolare riferimento al trattamento dei dati sensibili e giudiziari;

- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato. Per la gestione dei documenti informatici all'interno dell'AOO, il RPS fa riferimento alle norme stabilite dal responsabile del sistema informativo dell'AgID.

Componente della sicurezza

La componente organizzativa, fisica, logica e infrastrutturale della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte per l'erogazione del SdP. Nella conduzione del centro servizi destinato ad erogare il SdP, ci si adegua a quanto previsto nelle MMS.

Firma digitale

Per l'espletamento delle attività istituzionali l'amministrazione fornisce la firma digitale o elettronica qualificata ai soggetti da essa delegati a rappresentarla a vario titolo.
I kit di Firma Digitale di cui si avvale ARPAL sono dispositivi composti da un lettore USB e da una Smart Card. All'interno della Smart Card vengono rilasciati due certificati:

- il certificato di Firma qualificata che identifica il titolare e grazie al quale è possibile firmare documenti a valore legale;
- il certificato di autenticazione CNS (Carta Nazionale dei Servizi) che permette al titolare di accedere ai servizi online offerti dalla Pubblica Amministrazione.

Un File firmato digitalmente in formato .pdf assume l'estensione "signed.pdf". E' possibile scegliere tra due tipologie di firme:

- Firma PDF Basic (PADES), tradizionale Firma PDF, conforme alla Normativa Europea, compatibile con tutti i comuni reader disponibili per questo formato;
- Firma Pades BES, particolare tipo di Firma PDF "avanzata" in linea con la Normativa Europea, viene riconosciuta correttamente solo dalla versione 10 del software Adobe.