SEZIONE 6: IL SISTEMA DI PROTOCOLLO INFORMATICO

Indice della Sezione

Il sistema di protocollo informatico e gestione documentale di ARPAT è denominato *freedocs* e permette:

- la registrazione elettronica di protocollo,
- la segnatura,
- la classificazione dei documenti e la loro organizzazione in fascicoli,
- la memorizzazione e la gestione elettronica dei documenti,
- la ricezione e l'invio di documenti digitali e l'interoperabilità con altri sistemi di protocollo informatico tramite la posta elettronica certificata.

freedocs è lo strumento per la gestione dei flussi documentali nella fase corrente e per il controllo dell'intera massa documentaria dell'Agenzia, così come è imposto dalla normativa vigente. In particolare, attraverso *freedocs* è possibile gestire le problematiche legate all'organizzazione dei documenti in fascicoli, alla permanenza dei fascicoli nell'archivio, alla riservatezza della documentazione e di tutte le informazioni caratteristiche di un flusso documentale.
La gestione documentale include le attività legate alla creazione dei documenti e la loro aggregazione in fascicoli in modo da agevolarne la protocollazione, l'organizzazione, la ricerca e l'archiviazione a norma di legge.
La gestione elettronica dei documenti cartacei è realizzabile tramite l'acquisizione, diretta o indiretta, da scanner, in modo da ottenere una versione digitale del documento cartaceo.
La gestione elettronica dei documenti supporta i processi amministrativi in quanto consente di operare sul contenuto del documento per realizzare nuove versioni dello stesso pur mantenendo memoria delle elaborazioni precedenti.
L'integrazione con la posta elettronica certificata consente la dematerializzazione dei flussi documentali tramite la trasmissione di documenti elettronici e l'interoperabilità, ovvero la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente.

6.1 PRINCIPALI FUNZIONALITÀ DEL SISTEMA

Di seguito sono descritte le principali funzionalità del sistema di protocollo informatico e gestione documentale in uso presso ARPAT.
I manuali operativi per gli utenti e l'amministratore sono da considersi allegati esterni al presente Manuale e sono pubblicati aggiornati nella Intranet dell'Agenzia.

6.1.1 Funzionalità di accesso al sistema

L'accesso al sistema avviene tramite l'inserimento di username e password.
Le credenziali di accesso sono quelle del sistema centralizzato di autenticazione ldap.

6.1.2 Profilazione degli utenti

Il *profilo utente* è costituito dall'insieme delle autorizzazioni che abilitano differenti funzionalità dell'applicazione.
Se nessuna abilitazione è attivata, l'utente dispone solo dei diritti di accesso alle notifiche, di consultazione della rubrica mittenti/destinatari, di ricerca e di smistamento.
Le funzionalità a cui ogni utente può essere abilitato sono:

- Gestione documenti (permette di inserire un documento all'interno del sistema)
- Protocollazione in ingresso
- Protocollazione in uscita
- Protocollazione interna
- Annullamento protocollo

- Gestione PEC in ingresso
- Classificazione
- Fascicolazione
- Gestione del repertorio dei fascicoli
- Gestione registri di protocollo (generale e di emergenza)
- Gestione organigramma
- Gestione utenti e gruppi di condivisione
- Amministrazione di sistema

L'elenco degli utenti e delle relative abilitazioni è pubblicato all'interno del sistema di protocollo informatico e aggiornato in tempo reale.

6.1.3 Funzionalità di gestione documentale

Le funzionalità di gestione delle attività documentali consentono l'automazione delle attività caratteristiche del flusso documentale: ricezione/creazione, registrazione di protocollo, segnatura, classificazione, fascicolazione e smistamento.
freedocs gestisce il documento e ne consente l'aggregazione in fascicoli e sottofascicoli, gestendo anche l'entità fascicolo/sottofascicolo.
L'inserimento dei dati dei documenti e dei documenti stessi, siano essi informatici o informatizzati (cioè cartacei scansionati), è alla base della gestione documentale: l'insieme dei dati inseriti nelle attività del flusso documentale costituisce il *Profilo* del documento.
I dati che costituiscono il profilo del documento sono:

- la tipologia documentaria, l'oggetto, l'ufficio "proprietario", la data, il numero, l'indicazione di riservatezza ai sensi del D.Lgs196/2003 ed il tipo di supporto d'origine (cartaceo/digitale);
- gli eventuali allegati al documento principale;
- i dati di protocollazione;
- i dati di classificazione/fascicolazione.

Lo smistamento rappresenta il sistema di comunicazione interno e consente di notificare e porre all'attenzione degli altri utenti del sistema i documenti e le relative informazioni in modo da agevolare e velocizzare il lavoro.
È possibile smistare uno o più documenti ad uno o più uffici e/o ad uno o più utenti, anche tramite apposite liste di smistamento. È possibile anche inviare una nota di trasmissione diversa o uguale per tutti i destinatari della notifica.

6.1.4 Funzionalità di gestione elettronica dei documenti

freedocs gestisce i documenti digitali immessi nel sistema ed offre all'utente la funzionalità di versioning dei documenti e di acquisizione diretta da scanner.
freedocs consente l'associazione del file sia al documento principale che a tutti gli allegati al documento principale.
La modalità di associazione del file è la stessa per il documento principale e per gli allegati e consente di recuperare il file:

- da un documento *freedocs* (quindi già presente nel sistema)
- da file system (cioè da una qualunque cartella di rete o locale)
- da una specifica cartella condivisa (dalla quale poi il recupero avviene in maniera asincrona)
- da scanner

6.1.5 Funzionalità riservate al responsabile (RSP)

Il Responsabile del Servizio di Protocollo Informatico ha a disposizione, in aggiunta alle normali funzioni utente, le seguenti abilitazioni:

- Gestione sistema di classificazione
- Gestione tipologie di trasmissione
- Gestione tipologie di procedimento
- Gestione tipologie di oggetto
- Gestione tipologie documentarie
- Gestione ulteriori campi fascicolo

6.1.6 Il tracciamento delle attività documentali

Come richiesto dalla normativa in materia di sistemi di protocollo informatico e gestione documentale, *freedocs* tiene traccia di tutte le operazioni di modifica effettuate sui documenti. In particolare il sistema traccia:

- le attività di inserimento, protocollazione, classificazione, fascicolazione;
- le modifiche effettuate sui dati di profilo;
- le modifiche apportate agli allegati;
- le versioni del file principale.

Il tracciamento delle attività documentali dà accesso ai dati del documento segnalando le varie operazioni di gestione documentale che sono state effettuate sul documento, corredate di data, ora e autore dell'operazione. Vengono anche mostrate le operazioni di modifica effettuate sui dati del profilo del documento.
Il tracciamento degli allegati mostra le modifiche (inserimenti ed eliminazioni) che sono state apportate agli allegati al documento.
Il tracciamento delle versioni mostra le differenti versioni del file principale. L'ultima versione è sempre quella corrente.

6.1.7 Gestione fascicoli

Il fascicolo rappresenta l'elemento base dell'organizzazione dei documenti e del loro governo. Aggregare i documenti in un fascicolo significa creare il vincolo archivistico tra i documenti e "l'affare" o l'attività che li ha prodotti. In questo modo, indirettamente si legano tra loro i documenti afferenti ad uno stesso "affare". Per questo il fascicolo non è solo un contenitore di documenti ma rappresenta anche il legame concettuale presente tra i suoi documenti.
Per creare un nuovo fascicolo/sottofascicolo sotto una voce di titolario, è necessario specificare: l'ufficio (voce dell'organigramma) che ha la competenza sul fascicolo (di default è quello dell'utente che sta creando il fascicolo), l'oggetto del fascicolo e l'ubicazione del fascicolo. Sono proposti in visualizzazione la voce di titolario selezionata con le relative indicazioni di fascicolazione. Le indicazioni di fascicolazione consentono di standardizzare l'inserimento dell'oggetto del fascicolo in modo da facilitarne la successiva ricerca e consultazione.
Sempre in fase di inserimento di dati sono presenti, all'interno della maschera di creazione del nuovo fascicolo, degli ulteriori campi che consentono di gestire in maniera standardizzata delle informazioni aggiuntive alla descrizione del fascicolo. Tali ulteriori campi sono definiti e gestiti dall'amministratore del sistema.
I fascicoli gestiti dal sistema sono riconducibili a tre differenti categorie: fascicoli per Oggetto, fascicoli per Procedimento, fascicoli per Tipologia Documentaria. L'utente dovrà pertanto specificare, in fase di creazione del fascicolo, l'informazione relativa all'oggetto, al tipo di procedimento oppure alla tipologia documentaria al quale il fascicolo fa riferimento.

La specifica del tipo di fascicolazione associata ad una specifica voce del titolario è stabilita nel Piano di classificazione e non può essere modificata dall'utente.
Lo smistamento di un fascicolo, funzionalità del tutto analoga allo smistamento di un documento, trasmette al destinatario della notifica i diritti di lettura/scrittura sul fascicolo notificato (rispettivamente per competenza/conoscenza).

6.1.8 Funzionalità di ricerca

Le funzioni di ricerca permettono di individuare documenti e fascicoli attraverso un ampia gamma di parametri. Una volta effettuata la ricerca si potrà accedere direttamente ai documenti/fascicoli individuati.
Il menu ricerche consente di effettuare:

- La ricerca puntuale tramite il numero e l'anno di protocollo
- La ricerca documenti attraverso tutti i dati di profilo
- La ricerca documento in base all'oggetto dell'allegato
- La ricerca fascicoli attraverso tutti i dati di profilo
- La ricerca documenti tramite i dati di spedizione PEC

Qualunque ricerca ha come risultato un elenco di documenti o fascicoli che soddisfano il criterio impostato. In tale elenco (che può anche essere composto da una sola riga), cliccando sull'oggetto del documento o del fascicolo, si accede al relativo profilo.
L'opzione di *ricerca documento* permette di cercare un documento attraverso tutti i dati di profilo: dati di ricezione/creazione, dati di classificazione, dati di protocollazione e dati di smistamento del documento.
Analogamente, la ricerca di un fascicolo o di un sottofascicolo permette di individuare uno o più fascicoli a partire da una serie di parametri. I parametri della *ricerca fascicolo* sono: la voce di titolario (da selezionare come nella classificazione), il tipo fascicolo, l'oggetto del fascicolo, l'ufficio, l'anno di apertura, l'anno di chiusura, le indicazioni sulla riservatezza e le note. Inoltre è possibile eseguire la ricerca tramite i dati opzionali che vanno ad arricchire il profilo dei fascicoli/sottofascicoli e tramite l'ubicazione degli stessi. Nel risultato della ricerca è inoltre possibile ricercare e visualizzare anche i sottofascicoli gestendo l'opzione "Includi sottofascicoli".

6.1.9 Accesso alla documentazione

L'accesso a fascicoli e documenti viene assegnato tramite due distinte componenti:

- la prima stabilisce se l'utente ha accesso a documenti e fascicoli protetti da vincolo di riservatezza (ai sensi del Codice privacy D.Lgs 196/2003);
- la seconda componente stabilisce la visibilità dei documenti all'interno dell'Area Organizzativa Omogenea. Nel caso sia selezionata l'opzione Globale l'utente avrà accesso a tutti i documenti dell'Area Omogenea. Altrimenti vi è la possibilità di definire dei gruppi "trasversali" che consentono all'utente di vedere documenti e fascicoli prodotti e appartenenti a sottoinsiemi di unità organizzative definiti a seconda delle esigenze dell'AOO. In base a questa seconda componente il sistema consente ad ogni utente l'accesso a:
    - tutti i documenti e fascicoli di proprietà dell'ufficio dell'utente o di un ufficio a questo subordinato;
    - tutti i documenti e fascicoli di altri uffici al cui accesso l'utente è stato abilitato
    - tutti i documenti e fascicoli notificati all'utente oppure all'ufficio dell'utente oppure ad un ufficio al cui accesso l'utente è stato abilitato.

6.2 ARCHITETTURA DEL SISTEMA

Il sistema *freedocs* è composto da:

- un data base Oracle;
- un repository documentale su file system;
- un'applicazione web
- degli applicativi per la generazione dei registri giornalieri di protocollo, l'invio/ricezione tramite PEC, il recupero file da cartella condivisa e la gestione del repository che sono schedulati su un client applicativo;
- dei componenti software locali da installare sui client utente per l'acquisizione diretta da scanner, la firma digitale e la stampa etichette di protocollo.

Il data base è Oracle 11g.
Il repository documentale di freedocs è su file system ed è composto dalle seguenti raccolte di files:

- files del sistema documentale
- email pervenute nella casella istituzionale di posta elettronica certificata (PEC)
- ricevute di accettazione e conferma pervenute nella casella PEC istituzionale

L'applicazione web è scritta in parte in Classic ASP e in parte in ASP.NET e utilizza alcune librerie di terze parti per la verifica della firma digitale (Chilkat Crypt e ZapSign-SDK), l'upload di file (SoftArtisans FileUp Standard Ed.) e l'invio di email (EASendMail SMTP Component).
Il server web è un server Windows 2008 Server R2 con Internet Information Server 7.5 e .NET framework 4.5.

Gli applicativi centralizzati di:

- creazione del registro giornaliero di protocollo
- invio e ricezione di messaggi PEC
- recupero file da cartella condivisa
- monitoraggio delle cartelle del repository documentale

sono installati su un client applicativo Windows 7 Pro e schedulati per essere eseguiti con la cadenza necessaria.
L'applicativo "CreazioneRegistri" crea il registro giornaliero di protocollo. Utilizza le librerie EASendMail, log4net.
L'applicativo "PecMonitor" invia e riceve i messaggi pervenuti nella casella di posta certificata collegata al sistema di protocollo e utilizza le librerie software: EAGetMail, EASendMail, ZapSign-SDK, log4net. Il medesimo applicativo recupera inoltre, nel sistema documentale, i files presenti in un'apposita cartella di rete (condivisa fra tutti gli utenti) per i quali sia stata effettuata la richiesta di recupero.
L'applicativo "GestioneFiles" effettua il monitoraggio delle cartelle del repository documentale e, nel caso in cui contengano più di 5000 files, crea delle nuove cartelle e aggiorna i puntamenti a queste ultime sul database del protocollo. Utilizza le librerie EASendMail, log4net.
Gli applicativi centralizzati sono scritti in linguaggio C#.

Sul client utente viene utilizzato un browser web aggiornato (Google Chrome, Mozilla Firefox o Internet Explorer) e possono essere installati i seguenti componenti software:

- Acquisizione da scanner: per la gestione diretta dello scanner (locale o di rete purché dotato di driver twain)
- Stampa Etichetta: per la stampa delle etichette di protocollo
- Firma digitale: per la firma digitale di documenti inseriti in freedocs

L'applicativo "ScanClient" utilizza le librerie software Tiff to PDF COM/SDK (Adultpdf.com Inc) e LeadTools.
L'applicativo "StampaEtichette" non utilizza librerie software. I modelli di stampante di etichette supportati sono:
ELTRON TLP 2742
ZEBRA TLP 2844 e 2844-Z
ZEBRA GK420T
L'applicativo "Firma digitale" utilizza la libreria software ZapSign-SDK e log4net.
Gli applicativi client sono scritti in linguaggio C# ("Firma digitale") e Visual Basic 6.0 ("ScanClient" e "StampaEtichette").

6.3 SICUREZZA DEL SISTEMA

Per quanto concerne la gestione generale della sicurezza ai sensi del D.Lgs 196/2003 "Codice privacy", è vigente in ARPAT un "Documento Programmatico della Sicurezza (DPS)" nella sua attuale revisione 4 del 30/03/2011.
In tale documento, approvato con Decreto del Direttore generale n. 149 del 31/3/2011 e reperibile sul sito web istituzionale e nella Intranet dell'Agenzia, sono riportate, tra l'altro:

- la distribuzione dei compiti e delle responsabilità ai fini del trattamento dei dati (personali e non);
- l'analisi dei rischi che incombono sui dati;
- le misure adottate e da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- le misure minime di sicurezza da adottare in caso di trattamenti di dati personali affidati all'esterno.

Per tali argomenti si fa quindi riferimento a tale documento, ovvero ad atti che lo integrino o lo sostituiscano. Il DPS è pubblicato nella Intranet dell'Agenzia.

Per quanto riguarda l'utilizzo della posta elettronica, l'accesso a Internet, l'utilizzo degli strumenti e servizi relativi alle tecnologie dell'informazione e della comunicazione e le modalità per effettuare i trattamenti dati, è vigente un "Disciplinare ICT e trattamento dati" approvato con il Decreto del Direttore generale n. 147 del 28/4/2009.
Anche per questi temi si fa riferimento a tale disciplinare, ovvero ad atti che lo integrino o lo sostituiscano. Il Disciplinare ICT è pubblicato nella Intranet dell'Agenzia.

La documentazione tecnica sul sistema di protocollo informatico e gestione documentale è prodotta secondo gli standard di documentazione dei sistemi di ARPAT[1]. È pubblicata nella Intranet dell'Agenzia e mantenuta costantemente aggiornata.
In questa sede vengono analizzate la varie componenti del sistema e le misure di sicurezza esistenti o in fase di realizzazione al momento della stesura del presente Manuale.

[1] Esiste, ad esempio, una "scheda gestione" in cui sono riportate:

- le informazioni generali sul sistema e sue funzionalità, sulle tipologie di dati personali trattati
- la distribuzione dei compiti e delle responsabilità nella gestione e utilizzo del sistema
- l'organizzazione della formazione
- le eventuali criticità del sistema
- le misure di sicurezza
- le modalità di monitoraggio, manutenzione e aggiornamento del sistema

6.3.1 Sicurezza dei documenti informatici

Formazione dei documenti

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

- l'identificabilità del soggetto che ha formato il documento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- la registrazione di protocollo dei documenti informatici;
- l'accesso controllato ai documenti informatici;
- la conservazione e la leggibilità dei documenti nel tempo.

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 formati aperti, standard e documentati quali:

- PDF – PDF/A
- TIFF
- JPG
- XML - OOXML
- Open Document Format (.ods, .odp, .odg, .odb)
- TXT

I documenti informatici prodotti dall'AOO con altri prodotti di text editor devono essere convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard sopra indicati 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 e la sua integrità, il documento è sottoscritto con firma digitale.
Per attribuire una data certa ad un documento interno firmato digitalmente, e prolungarne quindi la validità oltre la data di scadenza del certificato, si assoggetta il documento al protocollo generale (entrata/uscita/interno).

Gestione dei documenti

L'architettura e le politiche di sicurezza dei sistemi informatici dell'Agenzia consentono l'accesso ai sistemi esclusivamente al personale addetto alla loro gestione.
Qualsiasi altro utente non autorizzato non può accedere ai documenti se non tramite *freedocs*.
La registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente avviene 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;
- garantisce 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.

Trasmissione dei documenti e interoperabilità dei sistemi di protocollo informatico

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono 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.
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 servizio di posta elettronica certificata del fornitore esterno (provider) di cui si avvale ARPAT è conforme alla normativa vigente in materia di posta elettronica certificata.
Per *interoperabilità* dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti.
Il sistema di protocollo informatico e gestione documentale di ARPAT integra la posta elettronica certificata e tramite questa interopera con altri sistemi di protocollo informatico.
La segnatura informatica che il sistema allega automaticamente a tutti i messaggi spediti tramite il sistema di protocollo è conforme alla Circolare n. 60 del 23 gennaio 2013 dell'Agenzia per l'Italia digitale ovvero alla sua versione più recente.

Accesso ai documenti

Il controllo degli accessi ai documenti del sistema è assicurato utilizzando le credenziali di accesso centralizzato ed un sistema interno di autorizzazione basato sulla profilazione degli utenti.
La profilazione consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo informatico e gestione documentale.
Il sistema di protocollo informatico e gestione documentale di ARPAT:

- 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;
- realizza il controllo delle autorizzazioni all'acceso ai documenti da parte degli utenti tramite apposite ACL;
- consente di associare un livello di riservatezza ai documenti trattati dall'amministrazione.

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.
Per maggiori dettagli si rimanda al paragrafo *Accesso alla documentazione*.

Accesso al registro di protocollo per utenti interni

Per gli utenti interni all'amministrazione/AOO, l'accesso ai registri di protocollo è regolata tramite un apposita abilitazione interna al sistema *freedocs*.
Sono abilitati alla gestione del registro di protocollo il RSP ed il suo vicario, il dirigente responsabile del Settore Affari generali e gli operatori dell'ufficio protocollo della Direzione generale.

Modalità di gestione delle utenze interne e dei relativi profili di accesso

Le richieste di attivazione o modifica delle abilitazioni devono essere richieste al RSP (o al suo vicario) da parte del Responsabile della struttura a cui l'utente è assegnato.

Accesso esterno

L'accesso al sistema di protocollo informatico e gestione documentale dell'Agenzia da parte di utenti esterni all'Agenzia non è consentito per motivi di sicurezza.
Per l'esercizio del diritto di accesso ai documenti ai sensi della Legge 241/1990, si rimanda allo specifico Regolamento interno vigente.

Conservazione dei documenti informatici

Per la conservazione a lungo termine dei propri documenti digitali ARPAT si avvale dei servizi dell'infrastruttura DAX - DigitalArchives eXtended per la conservazione degli archivi digitali, di Regione Toscana.

6.3.2 Sicurezza delle registrazioni di protocollo

Tutti i dati gestiti dal sistema di protocollo informatico e gestione documentale dell'Agenzia vengono registrati su data base.
Il data base del protocollo è accessibile direttamente solo agli amministratori di sistema e al RSP.

6.3.3 Gestione dei messaggi PEC ricevuti

Tutti i messaggi pervenuti nella casella istituzionale di posta elettronica certificata, ricevute comprese, vengono salvati in formato .eml su file system. Sono soggetti a backup e conservati per 5 anni. A seguito di tale salvataggio i messaggi vengono eliminati dalla casella PEC.

6.3.4 Gestione delle registrazioni di sicurezza (LOG files)

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) 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 da:

Log del sistema *freedocs*

Per ogni componente applicativa del sistema esiste un file di log:

- il log dell'applicazione web contiene la registrazione di tutte le operazioni effettuate sul sistema documentale da tutti gli utenti. Ogni giorno viene rigenerato un log e quello del giorno precedente viene zippato;
- i log degli applicativi CreazioneRegistri, PecMonitor, InvioEmail e CreazionePDF vengono generati sulla macchina in cui viene eseguito l'applicativo. Il log è composto da n files (parametro configurabile dell'amministratore di sistema) che vengono sovrascritti a rotazione;

- gli applicativi locali (Acquisizione da scanner, Stampa etichette e Firma digitale) generano log locali nel pc client in cui vengono eseguiti.

I log dell'applicazione web vengono conservati per 12 mesi. All'inizio di ogni anno vengono eliminati i log di due anni prima.

Log dei sistemi di sicurezza periferica

Per sistemi di protezione periferica del sistema di protocollo informatico si intende: Intrusion Detection System (IDS), sensori di rete e firewall.
I log dei sistemi di sicurezza vengono conservati per 12 mesi. All'inizio di ogni anno vengono eliminati i log di due anni prima.

6.3.5 Politiche di backup e conservazione

Tutti i server del sistema sono gestiti in housing presso il TIX, datacenter della Regione Toscana.
Le politiche di backup sono riportate nello specifico allegato al presente Manuale.

6.3.6 Continuità operativa e disaster recovery

I piani di continuità operativa e di disaster recovery dei sistemi informatici di ARPAT sono in fase di definizione e adozione.